Google Inc. et al v. Egger et al

Doc. 475 Att. 2

# Exhibit 13

Dockets.Justia.com

**John S. Pistole**
**Deputy Director**
**Federal Bureau of Investigation**

**American Bankers Association/American Bar Association**
**Money Laundering Enforcement Conference**
**Washington, D.C.**

**October 22, 2007**

# *"The FBI and the Financial Sector: Working Together to Protect our Citizens and our Economy"*

***Note: The Deputy Director may deviate from prepared remarks***

**DISSEMINABLE**

---

Good morning. It's an honor to be here today to talk about terrorist financing and how it affects the law enforcement business and the banking business.

Today I want to give you an overview of terrorist financing and walk you through the FBI's process of conducting terrorist financing investigations. And finally, I'd like to talk about how important all of you are to the FBI's counterterrorism mission.

* * *

Money is the lifeblood of terrorism. Without it, terrorists cannot train, plan, communicate, buy equipment, or execute their attacks. But with it, they can do immeasurable damage. And so they are always looking for ways to fly below the radar, hoping to stay unnoticed and unsuspected while they turn their plans into a reality.

We learned this lesson the hard way on September 11, 2001. The 9/11 hijackers wanted to remain unnoticed, and their financial transactions did fly below our radars. It wasn't until after the attacks—when we began backtracking through their finances—that red flags went up.

We discovered that the hijackers used the formal banking system freely and even shared access to accounts. We were able to track their everyday purchases at places like Wal-Mart and their travels throughout the country. Things that might not have registered before suddenly took on enormous significance. For example, they had no Social Security numbers. They moved their money in relatively small, non-suspicious amounts, using mainly wire transfers and credit and debit card transactions and some cash transactions.

But they didn't engage in any complex financial tradecraft to conceal their activities. Instead, they looked for weaknesses they could exploit. For instance, they sent structured wire transfers from institutions that had no software or program in place to detect them. One financier simply used an alias to wire money, because he knew the sending bank didn't have a robust "Know Your Customer" program.

Our financial investigation conclusively linked the hijackers together. But it is not enough to conduct a financial autopsy after an attack. It became clear that the law enforcement and intelligence communities needed to find early opportunities to identify and to disrupt terrorist networks. The best way to do that is to scrutinize finances.

When terrorists raise, store, move, and spend money, they leave trails. They are complex—but they are traceable and identifiable through global financial systems.

The financial analysis of the September 11 hijackers gave us a better idea of what to look for. It helped us establish new intelligence requirements and set up new tripwires. We established a specialized section in our Counterterrorism Division called the Terrorism Financing Operations Section, or TFOS.

The mission of our agents and analysts in TFOS is to trace transactions and track patterns. This painstaking work helps us identify, disrupt, and prosecute terrorists, their associates, their leaders, and their assets.

* * *

Let me give you a sense of how we conduct terrorist financing investigations and what we're looking for. But just a quick reminder that predication is the key to every investigation we undertake. We are not out looking at everyone's finances for no reason. In fact, when it comes to terrorist financing, it is often you who provide the predication for our investigations.

First and foremost, we're looking for basic personal information—addresses, birthdates, phone numbers, and employment. These help us understand day-to-day expenses and spending habits. This information then helps us uncover travel patterns, other accounts, important transactions, and financial histories. And these in turn may lead us to previously unknown business or personal associations, including other members of a network. They may also lead us to discovering criminal activity, such as IRS violations or money laundering.

In short, the most basic financial investigative techniques can result in a gold mine of intelligence.

But we don't want to do a financial autopsy after an attack has occurred. Instead we want to conduct proactive investigations—and we are.

For example, we investigate charities or non-governmental organizations that are used to generate and move money around the world. Some of them fraudulently obtain charitable donations and then divert them to support terrorism.

This was the case with the Benevolence International Foundation in Chicago. It claimed to provide relief to widows and orphans—and it did in fact use some of its funds to provide humanitarian assistance. But the organization was actually a front for al Qaeda. The Executive Director pled guilty to racketeering conspiracy and is now serving 11 years in federal prison.

We also investigate traditional criminal activity that might be used to support terrorism. Because of the crackdown on terrorists and their supporters, terrorists are not necessarily getting stipends from al Qaeda. Instead, they are raising it themselves, often through garden-variety crimes.

For example, the Madrid bombers sold drugs and pirated CDs. A group in North Carolina smuggled cigarettes and used the profits to fund Hezbollah in Lebanon. And in Torrance, California, members of a terrorist cell robbed gas stations so they could buy weapons and plan attacks against Jewish targets and U.S. military installations in Los Angeles. And so we must always be looking for links among traditional crimes and terrorist activities.

Another type of case is one in which we investigate facilitators—the people who move the money, whether witting or unwitting. In addition to using the traditional banking system, terrorists and their supporters also take advantage of unregistered Money Service Businesses and hawalas. These appeal to terrorists and their supporters for obvious reasons. One does not need to be an existing customer to use them.

Hawalas are informal remittance systems that operate primarily within ethnic communities. They can be operated from any location with a phone and Internet hookup, whether it is a gas station or a private home. They don't operate by any of the rules of the financial sector. There is no one to regulate anything. Hawalas are based on trust and offer near-anonymity for those who are trying to avoid scrutiny. In one case, we investigated a hawala that had sent approximately $4 million to over 20 different customers in foreign countries.

* * *

The 9/11 hijackers proved that terrorists and their supporters are always looking for chinks in the armor of our financial systems. We've made tremendous progress in the past six years in making it much harder for them to raise and move money. A big part of this is thanks to you.

Just like criminals and their money launderers, terrorists and their support networks rely on secrecy to conduct their business. If their activities can be monitored and flagged, they can potentially be stopped. We in the FBI can't do our jobs without the help and cooperation of the banking industry.

You are the gatekeepers of information about terrorists' financial activity. Your compliance with reporting requirements, subpoenas, and other requests for information are absolutely vital to our efforts.

The stronger our systems are, and the closer our coordination is, the better our chances at detecting and stopping terrorists before they can act.

Records produced and maintained pursuant to the Bank Secrecy Act are especially vital weapons in our arsenal—particularly Suspicious Activity Reports and Currency Transaction Reports. Every single one of our terrorism investigations has a financial sub-file—and one of the first things on our checklist is to query FinCEN for BSA reports that match the subject. You would be amazed at how much valuable intelligence they produce—especially SARs and CTRs.

As we have seen since the September 11th attacks, terrorists don't necessarily need huge sums of money to plan and carry out an attack. In a sample of FBI cases, about 42 percent of subjects had BSA reports filed. About 50 percent of those reports reflected transactions of $20,000 or less. This produces a vast amount of financial intelligence.

SARs highlight suspicious behavior and point us to indicators of potential criminal activity—such as structuring and other forms of money laundering. They may be the only hook we have to detect a terrorist cell.

CTRs help fill out the financial intelligence picture because of the objective criteria for filing them. Rather than a subjective analysis of financial behavior, they document specific transactions and patterns of activity that may be the crucial piece of evidence to a case.

CTRs actually provide financial intelligence on more subjects than SARs reporting alone. One tool is not a substitute for the other. SARs and CTRs work in concert together—and together, they are a powerful weapon. Obviously, they provide information about specific transactions. But they provide a much bigger picture than just isolated transactions. They fill in biographical or geographical information—which might let us prove where a suspect was on a particular day. They help us develop leads to expand our investigations. They can link people and accounts conclusively together—connections we might not otherwise see.

Let me give you an example. Some of you may have heard of the Al Haramain Islamic Foundation. It was a charity based in Saudi Arabia, with branches all over the world. Its U.S. branch was established in Oregon in 1997 and in 1999, it registered as a 501(c)(3) charity.

In 2000, the FBI discovered possible connections between Al Haramain and al Qaeda and began an investigation. We started where we often start—by following the money.

And we uncovered criminal tax and money laundering violations.

Al Haramain claimed that money was intended to purchase a house of prayer in Missouri—but in reality, the money was sent to Chechnya to support al Qaeda fighters.

In 2004, the Treasury Department announced the designation of the U.S. branch of Al Haramain, as well as two of its leaders, and several other branch offices. In 2005, a federal grand jury indicted Al Haramain and two of its officers on charges of conspiring to defraud the U.S. government.

We relied on BSA information and cooperation with financial institutions for both the predication and fulfillment of the investigation. Because of reporting requirements carried out by banks, we were able to pursue leads and find rock-solid evidence.

Yes, we used other investigative tools—like records checks, surveillance, and interviews of various subjects. But it was the financial evidence that provided justification for the initial designation and then the criminal charges.

That's why your cooperation is so vital—and that of the Treasury Department as well. As in the case I just discussed, together we have frozen the assets of at least 440 suspected and known terrorists or terrorist organizations. We couldn't have done this without the diligence and dedication of the financial institutions that carry out these designations. It is difficult to measure success in convictions of terrorist financiers because of the variety of violations we may use to charge suspects. But it is safe to say that any convictions we achieve absolutely depend on banking information.

So when your bank's officers are conducting reportable transactions, there are some things they can do to help us glean even more information right off the bat. Let me just run through a few:

- You can complete each applicable field.

- You can verify personal identifiers, where possible, and even complete the "description" narrative. When you fill out the "who, what, when, where, why, and how" on the front end, this saves us all time on the back end, because we don't have to come back to you with subpoenas, looking for specific information.

- You can check all the violation types that apply and avoid checking the "other" box.

- Finally, you can file the reports electronically, which will save all of us time.

- And if a customer strikes you as especially suspicious, call us in addition to filing a SAR.

Believe me, we know that this creates a lot of work for you. We also know you don't necessarily see an obvious return on your investment. But these reports do help us. They often become the cornerstones of our cases. Concrete connections are made by things as innocuous as learning the name of an account's co-signer. The more information we have, the more we have to go on. When we can follow the money, we stand a much better chance of breaking a case wide open.

All of this requires tremendous effort from us all—from your employees and from the FBI's employees. But this cooperation does more than just help us find terrorists and bring them to justice. It helps us all protect the integrity of financial institutions.

* * *

Before I conclude, I want to take a moment to talk about another area of risk, and another way that collaboration can help reduce that risk—and that is in the cyber arena.

We know that terrorists want to wreak havoc on our society, whether by outright attacks on our lives or attacks on our economy. One way in is through cyberspace. Your companies face external risks from terrorists hacking your systems and internal risks from trusted insiders.

We know that hackers have exfiltrated huge amounts of data from the systems of various companies and institutions. The U.S. government is taking strong steps to help shore up vulnerabilities in the .com, .gov, and .edu worlds, and we have identified a number of perpetrators and hardened a number of targets. But as you know, there are always those who are searching for still more vulnerabilities.

Yes, it is your responsibility to protect your systems, but we can help you. Our InfraGard program is a partnership between the FBI and private companies that works to help all of us protect our infrastructure. About two-thirds of Fortune 500 companies are represented, and if you're not a member, we urge you to become one. The InfraGard program lets us share information in a trusted environment on everything from computer intrusions to extortion. If we are all on the same page, we can work with you to investigate the source of the attack and help you guard against another one.

You also face threats from trusted insiders. What if al Qaeda or another foreign sponsor were able to infiltrate someone into your company, perhaps as an IT specialist or systems administrator? The FBI has certainly had a number of applicants for these jobs. Their goal is to get through our screening and get access to our systems. This would be just as dangerous as a truck bomb exploding. These insiders are sophisticated and must be closely watched. Otherwise, they could take down your system, compromise other companies, and cause grave and widespread economic damage.

We all want to protect the privacy of our clients and citizens, yet we also want to protect their security and their lives.

* * *

And so we need to continue our cooperation—and strengthen it. Because more challenges loom ahead, for all of us.

Globalization and technology present new complications. Stored value cards lack regulation and permit both anonymity and easy transportation of funds. Internet banking also opens up new channels for those wishing to make anonymous transactions. And online payment services don't have even basic customer identification and record-keeping regulations.

And on the opposite end of the technology spectrum, we expect to see cash couriers who can move money without the oversight your institutions provide.

Our adversaries will either become more technologically savvy or they will regress to methods that don't leave a paper trail. We can't predict what they will do. But we can do everything in our power to make it more difficult for them.

Tightening our financial systems works to our advantage and to our enemies' disadvantage. The more we work together, the more we deny them the ability to work in secret and force them to be creative. And the more they are forced to take risks and find ways around our systems, the higher the likelihood they will slip up.

And if they do, we will be waiting to catch them. The threat is real, and the stakes are high. We must not fail. And working together, we will not fail.

---

[Executive Speeches Index] [OPA Home]

Exhibit 14

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Lynne Bernabei, Esq.
The Bernabei Law Firm, PLLC
1775 T Street, NW
Washington, DC 20009-7124

VIA FACSIMILE

Thomas Nelson, Esq.
Box 1211
24525 E. Welches Rd.
Welches, OR 97067

FEB 06 2008

**Re: Al Haramain Islamic Foundation, Inc.-Oregon and Soliman al-Buthe**

Dear Ms. Bernabei and Mr. Nelson:

I write in response to Ms. Bernabei's letter of January 4, 2008, and in furtherance of our letter to you of November 14, 2007, which provided notice that OFAC was considering redesignating Al Haramain Islamic Foundation, Inc.-Oregon ("AHIF-Oregon") and Soliman al-Buthe. As set forth below, after a thorough investigation and review of the evidence in the record regarding AHIF-Oregon and Mr. al-Buthe, OFAC has determined that AHIF-Oregon and Mr. al-Buthe continue to meet the criteria for designation under Executive Order 13224 ("Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism") ("E.O. 13224") and, based on an updated and revised Administrative Record, including submissions by your clients, they are hereby redesignated. Accordingly, AHIF-Oregon's and Mr. al-Buthe's pending requests for delisting are denied. Separately, please see the last section of this letter for an update concerning OFAC policy on the use of blocked funds for the payment of legal expenses.

Redesignation

In reaching the decision to redesignate, OFAC has considered the following: (1) all communications between OFAC and your offices or other counsel on behalf of AHIF-Oregon and Mr. al-Buthe, including submissions made both prior to and following the original designation in September 2004; (2) a revised version of the initial designation memorandum and supporting exhibits; and (3) additional unclassified, privileged, and classified information. As you have requested, all of the submissions you have made on behalf of AHIF-Oregon and Mr. al-Buthe have been incorporated into the Administrative Record. The additional unclassified material OFAC has obtained and reviewed in response to AHIF-Oregon's petition for reconsideration (in addition to the unclassified material upon which the original designation was based) has been provided to you previously and will also be available to you in the course of the litigation associated with this matter.

Your arguments related to why AHIF-Oregon should not be designated pursuant to E.O. 13224 primarily consist of the following:

- AHIF-Oregon was an independent organization that was involved exclusively in charitable activities and was not involved in the support of terrorism, Specially Designated Global Terrorists, or other alleged supporters of terrorism;
- AHIF-Oregon funds transferred to AHIF in Saudi Arabia for use in Chechnya were not used to support terrorism, but rather in support of AHIF/Saudi Joint Relief Committee activities in Chechnya that were approved of by the Russian Government;
- AHIF-Oregon's distribution of Islamic literature was constitutionally protected activity and not an appropriate basis for designation.

After considering your arguments and submissions, and reviewing the whole Administrative Record, I have determined that the Administrative Record compiled by OFAC provides reason to believe that AHIF-Oregon meets the criteria for designation pursuant to E.O. 13224 on the following bases: (1) being owned or controlled by SDGTs Aqeel al-Aqil and al-Buthe, (2) acting for or on behalf of SDGTs al-Aqil and al-Buthe, and (3) supporting and operating as a branch office of AHIF, an international charity that employed its branch offices to provide financial, material, and other services and support to al Qaida and other SDGTs.[1] Among the information relating to AHIF-Oregon supporting the redesignation is the fact that two of the founding directors of AHIF-Oregon were — and remain — Specially Designated Global Terrorists, namely Mr. al-Buthe, who was the Treasurer of AHIF-Oregon, and Mr. al-Aqil, who was the founding President of both AHIF-Oregon[2] and AHIF in Saudi Arabia. Both classified and unclassified reporting indicates that the AHIF parent organization in Saudi Arabia, and in particular Mr. al-Aqil himself, maintained strong and direct control over activities of the branches. Mr. al-Aqil himself confirmed in a 2002 interview that the AHIF parent organization in Saudi Arabia maintained "tight control" over its branches.

Substantial classified and limited unclassified reporting, including the Staff Report to the National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing that Ms. Bernabei provided to OFAC in 2004 for consideration, reveals the extent and nature of AHIF's longstanding and significant support, through its international branches, of SDGTs and terrorist activity around the world, including al Qaeda and the mujahideen in Chechnya, and dating back as far as the 1998 bombings of the U.S. Embassies in Kenya and Tanzania. AHIF-Oregon was an active arm of this worldwide organization, and its operations, including its direct provision of funding to AHIF in Saudi Arabia,[3] enabled the global AHIF to continue supporting terrorist activities. Finally, your arguments regarding AHIF activities in Chechnya were considered, but rejected in light of the classified and unclassified administrative record.

---

[1] AHIF-Oregon's distribution of Islamic literature is not a basis upon which AHIF-Oregon has been redesignated, nor was it a basis for the designation in September 2004.

[2] As set forth in Ms. Bernabei's correspondence of August 4, 2004, Mr. al-Aqil and another senior al Haramain official, Mansur al-Kadi, purportedly submitted formal resignations from the AHIF-Oregon board in 2003. Nevertheless, classified and unclassified information indicates that Mr. al-Aqil retained effective control over the activities of all branches until his departure from AHIF in 2004, and according to some reports, even following his purported departure from the parent organization.

Additional Issues Raised by AHIF-Oregon

I would also like to respond to several concerns raised in Ms. Bernabei's January 4, 2008 letter.[4] First, Ms. Bernabei indicates that there is no basis in E.O. 13224 or the applicable regulations for a redesignation. A redesignation is, in essence, a process whereby OFAC updates and supersedes its original designation on the basis of a revised administrative record. OFAC undertakes the redesignation process pursuant to the same standards as apply to any designation action under E.O. 13224. Specifically, OFAC analyzed the applicability of designation criteria set forth in section 1 of the E.O. based on all information currently available to it. OFAC also provided AHIF-Oregon notice of the pending determination and allowed AHIF-Oregon to provide any additional information it wished OFAC to consider. In the end, this redesignation has provided more process for the benefit of AHIF-Oregon than would have been provided were OFAC simply to have amended the original designation record administratively, which, as Ms. Bernabei points out, the OFAC regulations provide for.

In sum, we are confident that the redesignation process — particularly when considered in light of the extent of materials provided to you by OFAC during the original designation process, as well as the willingness of OFAC to accept numerous submissions from AHIF-Oregon for consideration and incorporation into the administrative record — has provided AHIF-Oregon with a constitutionally sound level of due process, as several courts have found in analogous circumstances. *See Holy Land Found. v. Ashcroft*, 219 F. Supp. 2d 57, 77 (D.D.C. 2002), *aff'd* 333 F.3d 156, 163 (D.C. Cir. 2003); *Islamic American Relief Agency v. Unidentified FBI Agents*, 394 F. Supp. 2d 34, 49 (D.D.C. 2005), *aff'd in part and remanded*, 477 F.3d 728 (D.C. Cir. 2007); *Global Relief Found., Inc. v. O'Neill*, 207 F. Supp. 2d 779, 804 (N.D. Ill. 2002), *aff'd*, 315 F.3d 748 (7th Cir. 2002). Of particular note, the Holy Land Foundation raised claims nearly identical to those in Ms. Bernabei's letter when it challenged OFAC's redesignation. The court rejected these arguments and upheld the redesignation. *See Holy Land Found.*, 219 F. Supp. 2d at 76, n.29.

Second, the January 4 letter also raises concerns about the unclassified, non-privileged materials provided to you. Specifically Ms. Bernabei asserts that not every exhibit pertains to AHIF-Oregon or AHIF in Saudi Arabia. OFAC is entitled to consider the full panoply of relevant information available to it, and all the information provided to you either relates directly to AHIF-Oregon or AHIF or provides context for such other information. *Cf. Holy Land Found.*, 333 F.3d at 162 ("it is clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations"). Moreover, OFAC is aware of the concerns presented by any media reporting, foreign and domestic, and considers the reliability of such reporting when relying upon such information.

---

[3] Both Ms. Bernabei's correspondence of September 21, 2005, and the Complaint filed challenging AHIF-Oregon's designation, admit such direct funding of AHIF in Saudi Arabia. *See. e.g.*, Compl. ¶ 63.

[4] As this matter is currently in litigation, this letter only touches upon several of the matters raised in the January 4 correspondence. OFAC reserves the right to provide responses in the litigation to any arguments raised by AHIF-Oregon in the litigation.

In many cases, the media reporting provided to AHIF-Oregon has been used in conjunction with classified materials. OFAC's use of classified information is provided for by statute and has been upheld by numerous courts. *See* 50 U.S.C. § 1702(c); *Global Relief Found. v. O'Neill*, 207 F. Supp. 2d 779, 791 (N.D. Ill.), *aff'd*, 315 F.3d 748, 754 (7th Cir. 2002); *Islamic American Relief Agency v. Gonzales*, 394 F. Supp. 2d 34, 45 (D.D.C. 2005), *aff'd* 477 F.3d 728 (D.C. Cir. 2007); *Holy Land Found. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003).

Third, OFAC and the Department of Justice requested that each agency that provided classified information used by OFAC in the redesignation process review that information to determine whether it remained appropriately classified. After several months of close coordination with multiple agencies, OFAC has been informed that, as of the date of this letter, all classified material used in the final Administrative Record remains properly classified.

In sum, as stated above, AHIF-Oregon and Mr. al-Buthe are thus redesignated, and all pending requests for delisting are hereby denied. This constitutes final agency action on this matter. A copy of the unclassified version of the evidentiary memorandum will follow shortly under separate cover.

Use of Blocked Funds for Legal Expenses

Regarding the use of blocked funds for payment of legal expenses, OFAC has recently adopted a policy to authorize the release of a limited amount of blocked funds for the payment of legal fees and costs under certain circumstances. Specifically, the policy would allow a limited amount of blocked funds to be released for the payment of legal fees and certain costs incurred in seeking administrative reconsideration or judicial review of the designation of a U.S. person pursuant to the Global Terrorism Sanctions Regulations, 31 C.F.R. Part 594. Accordingly, the policy would potentially apply to your representation of AHIF-Oregon.

In order to complete the processing of your license request(s) pursuant to this policy, OFAC requests the following information:

- The hourly rate and number of hours billed per attorney for legal services directly related to the request for administrative reconsideration of the designation and the legal challenge thereto, divided by each phase of the case (i.e., administrative filings to OFAC and proceedings at the district court);

- An itemized statement and description of costs incurred in seeking administrative reconsideration or judicial review of AHIF-Oregon's designation;
- A certification, signed under penalty of perjury, that AHIF-Oregon has no assets, property, or economic resources of any type outside the United States, and does not have access to any AHIF funds worldwide; and
- A certification that to the best of your knowledge the blocked funds do not represent the property interest of another or serve as security for other obligations of AHIF-Oregon.

OFAC will evaluate your request(s) for the release of blocked funds for payment of attorney fees and costs incurred in seeking administrative reconsideration and judicial review of AHIF-Oregon's designation pursuant to the policy upon receipt of the information requested.

Sincerely,

Adam J. Szubin
Director
Office of Foreign Assets Control

Exhibit 15

PANEL ONE OF A HEARING OF THE SENATE JUDICIARY COMMITTEE SUBJECT: FISA FOR THE 21ST CENTURY CHAIRED BY: SENATOR ARLEN SPECTER (R-PA) WITNESSES: GENERAL MICHAEL HAYDEN, DIRECTOR, CENTRAL INTELLIGENCE AGENCY; LT. GENERAL KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY; AND STEVEN BRADBURY, ACTING ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL COUNSEL, DEPARTMENT OF JUSTICE LOCATION: 226 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C. TIME: 9:00 A.M. EDT DATE: WEDNESDAY, JULY 26, 2006

---

SEN. SPECTER: (Sounds gavel.) Good morning, ladies and gentlemen. The Judiciary Committee will now proceed with our hearing on the proposed legislation which would submit the surveillance program for constitutional review to the Foreign Intelligence Surveillance Court.

Wiretapping has been going on in the United States involving U.S. citizens some four and a half years without having the traditional judicial approval. Since it was publicly disclosed in mid-December, the Judiciary Committee has held five hearings and has considered a variety of proposed bills, leading to the legislation which we have before us today, which has been meticulously negotiated and has the agreement of the president to refer the surveillance program to the FISA Court, if the legislation is approved. There may be modifications, subject to the agreement of the president.

The Foreign Intelligence Surveillance Court is well-suited to handle this review because of its expertise in the field and because of its secrecy, with insistence by the White House that there not be public disclosures.

Moving to the substance of the bill, I first want to take up two items where critics do not face reality on these two major points. First, there is a contention that the bill is defective because it does not retain the Foreign Intelligence Surveillance Court as the exclusive place to determine wiretapping. The reality is that since the president has put his program into effect, the Foreign Intelligence Surveillance Act, administered by the Foreign Intelligence Surveillance Court, is in fact not the exclusive remedy. The president claims that he has inherent Article II power to conduct wiretapping aside from the court.

Three appellate courts appear to agree with that, but it depends upon what the program is. The constitutional requirements are that there has to be a balancing of the value to security contrasted with the incursion into privacy, and that can only be determined by judicial review. And in a context where the president is demonstrably unwilling to have the program subjected to public view, it would have to be determined by the FISA Court if it is to be ruled on constitutionally at all.

The second point where the critics are objecting, which I submit does not face the reality, is the contention that the proposed legislation expands the Article II power of the president of the United States. A statute cannot do that. The constitution is supreme. If the president has the constitutional authority under Article II, that supersedes the statute, and a new statute may not add or diminish the president's constitutional power.

The legislation has received a considerable amount of commentary, a considerable amount of critical commentary, and candidly, I welcome the dialogue because I am personally convinced that when the legislation is fully understood and we -- faced with the reality of this surveillance going on, unchecked.

constitutionally in the absence of any better way to do it -- when this legislation is fully understood with those factors, there will be acceptance.

The commentary today in one of the major papers says that the legislation adds a provision, quote, "Nothing in this act shall be construed to limit the constitutional authority of the president to collect intelligence with respect to foreign powers and agents of foreign powers." Well, this bill doesn't add that. That provision is in the current Foreign Intelligence Surveillance Act. And it is there because it deals with embassies, foreign embassies, foreign residences of people of the United States representing foreign governments, and there has never been a requirement that there would have to be court approval to have wiretapping in that situation.

The commentary today says that the bill explicitly acknowledges an alternative source of power. Well, the bill doesn't. Article II power is what it is.

Now, I would have preferred to have had some other provisions, candidly. I would liked to have had the program mandatory so that the president would have to submit it to the FISA Court. But I could understand the president's refusal to do that in light of his being unwilling to bind future presidents and make an institutional change in what powers the president has.

My goal is to solve the current problem. The president has made a firm commitment to me, later confirmed by his White House personnel publicly, a firm commitment -- may the record show that Mr. Steven Bradbury, who negotiated for the president, is nodding in the affirmative -- made a firm commitment to submit the program to the FISA Court.

Now, I would like to have a mandate, but this president is not going to give a mandate and yield to that kind of legislative authority. And even if the statute did provide a mandate, if a future president challenges it under Article II powers, Article II powers are what they are, and the statute could not bind a future president.

It really seems to boil down to me in many quarters that if the president agrees with it, there must be something wrong with it. There is a widespread sense that there is something amiss with presidential agreement. Well, this legislation was negotiated in a way that I have characterized as fierce, and when we come to Mr. Steven Bradbury, the acting assistant attorney general for the Office of Legal Counsel, we'll get into some of the details on that.

In light of the president's commitment, I think it is fair to say that this legislation is a breakthrough. Today's commentary refers to other bills which are pending; some by members of the Intelligence Committee who know the details of the program. Well, none of the bills does what this bill does. None of the bills reaches judicial review of the program.

We've had two recent decisions by United States District Courts. Last week, the chief judge of the District Court in San Francisco, Judge Walker, made a determination that a suit, Hepting versus AT&T, would go forward, but a close reading of that 72-page opinion shows it goes forward under very limited ways. And Judge Walker has put so many hurdles on state secrets that it is highly doubtful that that case will last much longer. Yesterday, a federal judge in

Chicago, Terkel versus AT&T, dismissed the case on grounds of state secrets. And when you read those cases, the obstacles are enormous.

If there is a sense to modify the provision in the legislation which gives exclusive jurisdiction to a FISA Court, that can be done. We wouldn't have the president's commitment, but the president talked about making modifications subject to his approval.

There are a number of changes which modernize the FISA Court, which we'll get into. I've talked longer than I customarily do, but I've done so because of the complexity of this issue and what, at least I think, is the lack of understanding of the legislation and its applicability.

We started a little early today because the prime minister of Iraq is scheduled to address a joint session at 11, and we may lose members by that time, and we also have a vote scheduled at 10:00. I'm pleased now to yield to the distinguished ranking member, Senator Leahy.

SEN. PATRICK LEAHY (D-VT): Well, I have -- thank you, Mr. Chairman. Thank you for convening this hearing, especially glad to welcome General Hayden, his first appearance before this committee since he assumed his new duties. I spoke with the general yesterday and told him how pleased I was to see the level of professionalism that he has brought to the agency and the appointments he's been -- made.

"Independence" and "competence" were the two watchwords that led me to believe that he'd serve well as the director of the CIA, and I said so at the time I voted for his confirmation. And again, we need some straight talk today in navigating this very difficult issue.

There are two sets of issues relating to the Foreign Intelligence Surveillance Act that are now before this committee. First, what is the extent of the administration's warrantless wiretapping in violation of FISA? And how should we in Congress react?

After seven months and four hearings, we remain largely in the dark about what the administration is doing and continues to do, because the administration has stonewalled this committee's bipartisan efforts at oversight.

But the answer is clear. We must demand and we must ensure that this administration and the next administration, which will follow in two and a half years, actually follows the law.

Does the FISA law itself need to be revised? It's been amended six times, at this administration's request, in the five years since 9/11. But even though we've done that six times at the administration's request, they now say it needs modernization. And that modernization is the focus of today's hearing. The Democratic members of this committee asked for such a hearing, and I compliment the chairman in having it.

But the issues of compliance and modernization are completely separate issues. Whether or not FISA needed fine-tuning is a legitimate consideration, but FISA's possible imperfections provide no excuse for the administration's flouting of existing law.

By the same token, the Bush-Cheney administration's outrageous disregard for existing law does not mean that we in Congress should shrink -- shirk our responsibility to improve the law if there's need to. So I'm ready to consider Section 9 on its merits, but I have serious grounds for skepticism.

If Section 9 revisions are, as claimed, needed to bring FISA up to date with 21st technology, why haven't we heard about them before now? I said we've amended it five times at the administration's request. In July 2002, former General -- Attorney General Ashcroft testified that the 2001 Patriot Act had modernized our surveillance tools to keep pace with technological changes. And in March of this year, in the reauthorization of the Patriot Act, we made all the amendments to FISA that the administration requested. In fact, the president then took credit for updating the law.

So if FISA as amended is too quaint to meet the challenge of the 21st century, then the Bush-Cheney administration owes the Congress and the American people an explanation of why they didn't speak up before now.

Now, to the extent I've been able to figure out the highly complex language of Section 9, it seems to me to permit vast new amounts of warrantless surveillance to telephone calls involving American citizens. It would appear to authorize unrestricted, unregulated government surveillance of American citizens talking to relatives, colleagues, trading partners overseas, without any showing that that's necessary to protect our national security.

But to the extent that the administration's witnesses can explain to us today, in practical and concrete terms, why these make sense, I'll listen. So I have some questions about it.

But let me turn to the rest of the bill. It's been called a compromise. Well, this Vermonter does not believe that we should ever compromise on requiring the executive to submit to the rule of law, no matter who is president.

And I'm sad to say that I see bill less as a compromise and more as a concession. It would abandon our oversight role, confine oversight to a single judge, on a secret court, whose decision on the one program the Bush-Cheney administration has agreed to submit for review is appealable only by the Bush-Cheney administration.

And even that oversight would not be required by the bill itself.

I know the chairman got the best deal he could. The president, the vice president, their legions, can be hard-headed rather than flexible bargainers. I make these observations respectfully, but also to express my reluctance to compromise FISA and the minimal protections, the minimal protections it provides for Americans. Section 8 would repeal FISA's exclusivity provision and affirmatively embrace the president's claim of sweeping inherent authority. The result is to make FISA optional. The president can use it or not use it, at his option.

So it's astounding that we're considering this proposal. FISA was never intended to give presidents choices; it was enacted to prevent abuses of executive power and protect Americans' liberties by prohibiting the government from spying on its citizens without court approval. The Bush-Cheney administration has chosen to simply ignore it. And I am wondering now if we are going to reward its flouting of the law by saying, in effect, "Oh, please excuse us for passing that law; we didn't mean to; we didn't expect you to follow it; we'll never do that again." That's like arresting a burglar with three bags of cash and saying, "Well, leave one bag here and we'll all be okay with that."

Defenders of the bill have argued that Section 8 is meaningless because the president has whatever constitutional authority the Constitution says and Congress cannot limit that authority through legislation. If the best we can say on behalf of proposed legislation is it's a waste of ink, then we shouldn't be enacting it. But I don't believe that.

When it goes to the secret FISA Court, the administration will adhere to the position that Section 8 is meaningless, and the administration is insisting on that for a reason. The Supreme Court recently explained in its Hamdan decision, the constitutional scope of presidential power depends on the legislation Congress has enacted, even in times of war. The Constitution grants Congress the express power to set rules for the military and express power to make all laws which shall be necessary and proper for carrying into execution all the powers vested by the Constitution in the federal government, including those of the president. In the absence of congressional action, the president may well have some measure of unilateral authority. That is what the president's -- the administration always cites -- (suggests ?). But once Congress acts, as it did in FISA, the president's no longer free to do whatever he wants to do. As the court said in Hamdan, whether or not the president has independent power absent congressional authorization, Congress, of course, may place limitation on those powers. That was the whole point of FISA, to limit the president's power to spy on ordinary Americans by making FISA the sole means by which foreign intelligence wiretaps may be conducted in the United States.

Waiving FISA's exclusivity provision would not be meaningless; it would completely gut FISA. It would give the president a blank check to carry out warrantless wiretapping whenever he chooses or whenever the next president chooses. I could not in good conscience acquiesce in such a sweeping signing away of Americans' liberties in any circumstances, and I'm certainly not going to do it at the behest of an administration that has continuously broken the law.

Thank you, Mr. Chairman. I'll put my full statement in the record.

SEN. SPECTER: Thank you, Senator Leahy.

Would any other members like to make an opening statement? (No response.)

Then we'll turn to our first witness, the distinguished director of the Central Intelligence Agency, General Michael Hayden. General Hayden comes to this position with a very distinguished record. He received his bachelor's degree from Duquesne University, 1967, master's also from Duquesne, in modern American history. We have not only an intelligence officer but a renaissance man with us here today. Since, of course, worked in the Armed Forces Staff College, the Air War College, Defense Intelligence School. He's had ranking positions, which we'll include in the record. He's had many awards, honors, which we will include in the record, and one we will note specifically is that he's a Pennsylvanian from Pittsburgh.

That is too important just to be included in the record.

MR. HAYDEN: Thank you, Senator.

SEN. SPECTER: We're honored, General Hayden, that you would testify before this committee on your first occasion since becoming director of the Central Intelligence Agency, and we look forward to your testimony.

MR. HAYDEN: Well, thank you, Mr. Chairman, Senator Leahy. Thanks for the opportunity to speak before your committee today.

The work that you and we have before us is truly important. How do we best balance our security and our liberty and continue the pursuit of valuable foreign intelligence?

Let me congratulate the committee for taking on the task of examining and, more appropriate, amending the Foreign Intelligence Surveillance Act.

This task of balancing security and liberty is one that those of us in the intelligence community take very seriously, and, frankly, it's one to which we turn our attention every day.

If I can be permitted one anecdote -- within days of the 9/11 attacks, I actually addressed the NSA workforce -- at the time, I was the director of that agency. It was a short video. I was talking to an empty room, but the video was beamed to our workforce throughout Fort Meade and globally, and most of what I said was what you would normally expect at a moment like that. I tried to inspire, our work was important, the nation was relying on us. I tried to comfort, look on the bright side -- a quarter billion Americans wish they had your job today. And I ended the talk by trying to give some perspective. I said all free peoples have had to balance the demands of liberty with the demands of security, and historically, we Americans had planted our flag well down that spectrum towards liberty. And so I ended my talk by simply saying here was our challenge. "We at NSA, we're going to keep America free," I said, "by making Americans feel safe again."

Now, that was not an easy challenge. The Joint Inquiry Commission, which I think most of you know was comprised of the House and Senate Intelligence Committees, would later summarize our shortcomings in the months and years leading up to the September 11th attacks. The commission -- sometimes harshly -- criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me just quote from some of the JIC -- the Joint Inquiry Commission's systemic findings, and here I'm quoting: "NSA's cautious approach to any collection of intelligence relating to activities in the United States" -- and again, I'm quoting -- "there were also gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." And again, NSA did not want to be perceived as targeting individuals in the United States.

And finally -- and here, the commission was talking about one-end U.S. conversations; by that, I mean conversations in which one of the communicants was in the United States of America -- the commission said there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist-related communications, at least in terms of protecting the homeland.

Now, for NSA, the challenge is very acute. NSA intercepts communications, and it does so for only one purpose -- to protect America, to protect the lives, the liberties and the well-being of the citizens of the United States from those who would do us harm. And by the late 1990s, that had become increasingly difficult. The explosion of modern communications in terms of volume, variety and velocity threatened to overwhelm as an agency.

The September 11th attacks exposed an even more critical and fundamental fault line. The laws of the United States do and should distinguish between the information space that is America and the rest of the planet. The laws of the United States do and should distinguish between the information space that is America and the rest of the planet. But modern telecommunications do not so cleanly respect that geographic distinction. All of us exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor.

What does place mean when one is traversing the Internet? There are no Area Codes on the World Wide Web.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3,000 of our countrymen from within the homeland. In terms of both technology and the character of our enemy, "in America" and "of America" were no longer synonymous.

I testified about this challenge in open session to the House Intel Committee in April of 2000. At the time, I used a metaphor, an example, and I created some looks of disbelief when I said that if Osama bin Laden crossed the bridge from Niagara Falls, Ontario, to Niagara Falls, New York, there were provisions of U.S. law that would kick in and offer him some protections and would actually affect how NSA could not cover him.

Now, at the time, that was just a stark hypothetical. Seventeen months later, after the attacks, that was the reality we were facing.

The legal regime under which NSA was operating, the Foreign Intelligence Surveillance Act, had been crafted to protect American liberty and American security. But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And frankly, I don't think anyone can make the claim that the FISA statute was designed to deal with a 9/11 or to deal with a lethal enemy who likely already had armed combatants inside the United States.

Because of the wording of the statute, the government looks to four factors in assessing whether or not a court order is required before NSA can lawfully intercept communication. And again, you won't find these articulated as such in the statute, but the impact of the statute is that we look to four things so that we can decide whether or not a court order is needed before NSA does what it does routinely. And those factors are: Who's the target? Where is the target? How do we intercept the communication? And where do we intercept the communication?

And frankly, Mr. Chairman, the bill before the committee today effectively re-examines the relevance of each of those factors and examines the criteria we now want to use going forward to use each of them.

Let me just talk about each of them for a moment. Who is the target? The FISA regime from 1978 onward focused on specific court orders against individual targets, individually justified and individually documented. That was well suited to a stable foreign entity on which we wanted to focus, for extended periods of time, for foreign intelligence purposes. It is not as well suited to provide the agility to detect and prevent attacks against the homeland.

Looked at another way, FISA's careful individualized processes exact little cost when our goal is long-term surveillance and exhaustive intelligence coverage against a known and recognizable agent of a foreign power. The costs are different when our objective is to detect and prevent attacks. The costs are different when we are in hot pursuit of communications entering or leaving the United States involving someone we believe to be associated with al Qaeda.

Now, in this regard, extending the period for emergency FISA to seven days and allowing the attorney general to delegate his authority to grant emergency orders is very welcome, and I believe very appropriate. So, first of all, who is the target?

Secondly, where is the target? As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available band width available each nanosecond, should our statutes presume that all communications that touch America be equally protected?

As the chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that happen to get routed through U.S. facilities. Frankly, I think our limited resources should focus on protecting U.S. persons, not those entities who might get covered as a result of technological changes that have extended the impact and then the protection of FISA far beyond what its drafters could ever have intended.

I know that Senator DeWine, among others, has been concerned about the allocation of these resources and FISA backlogs. And frankly, now, as director of CIA, who must provide the predicate for FISA orders, I share his concerns in allocating resources and hope the legislation will help us properly focus resources on protecting the legitimate privacy rights of U.S. persons.

Now, beyond who and where is the target, there's the question of how do we intercept the communication. For reasons that seemed sound at the time of enactment, the current statute under which we operate makes a distinction between collection on a wire and collection out of the air.

Now, when the law was passed, almost all local calls were on a wire and almost all long-haul communications were in the air. Now, in an age of cell phones and fiber optic cables, that is totally reversed, with powerful and unintended consequences for how NSA can lawfully acquire a signal.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should you. My view is that the statute we develop should be technology-neutral.

And then, finally, beyond how do we intercept the communication, there's the question of where. Where do we intercept it? A single communication can transit the world even if the communicants are only a few miles apart. That happens routinely. And in that transit, NSA may have multiple opportunities to intercept it as it moves and as it changes medias.

As long as a communication is otherwise lawfully targeted, I believe we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, particularly in today's telecommunications universe. Intercept of a particular communication, one that would help protect the homeland, for example, is always probabilistic. It is never deterministic. No coverage is guaranteed. We simply need to be able to use all the technology tools we have.

In that light, as I said earlier, there are no communications more important to the safety of the homeland than those affiliated with al Qaeda, with one end of the communication in the United States. And so why should our laws make it more difficult to target the al Qaeda communications that are most important to us, those entering or leaving this country?

Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge. We also need to protect that edge, and we need to protect those who provide it to us.

The proposed legislative language that requires compulsory compliance from carriers is a very important step in this regard. After 9/11, patriotic Americans from all walks of life assisted us, the intelligence community, in ensuring that we would not have another attack on our soil. Even prior to 9/11, we received critical assistance across the intelligence community from private entities.

As director of NSA, as deputy DNI, now as director of CIA, I understand that government cannot do everything. At times we need assistance from outside government.

Whatever legal differences and debates may occur about separations of power, Article II and other critical and very important issues, those people who help to protect America should not suffer as a part of this debate. I would urge the committee to recognize the importance of those efforts to these Americans and provide appropriate protections.

One final and very important point. Many of the steps contained in the proposed legislation will address the issue raised by the Congressional Joint Inquiry Commission -- back again -- one-end U.S. conversations, communications that that commission characterized as, again quoting, "among the most critically important kinds of terrorist-related communications." That means my friend here, General Alexander and his agency, NSA, will bump up against information to, from or about U.S. persons. Let me stress that NSA already routinely deals with this challenge and knows how to handle it while protecting U.S. privacy.

I was very happy to note that the draft bill contains quite a bit of language about minimization and minimization procedures. Minimization is the process that NSA uses to protect U.S. privacy, to protect U.S. identities. The same rules of minimization that NSA now uses globally, rules that are approved by the attorney general and thoroughly briefed to Congress, will be used under any activities that are authorized by the pending legislation.

Let me close by saying that we have a great opportunity here. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you very much. And I know my colleagues have opening statements, but after them I'd be very happy to take questions.

SEN. SPECTER: Thank you very much, General Hayden.

We now turn to General Alexander, who is now the director of the National Security Agency. His bachelor's degree is from West Point, master of science in business administration from Boston University, master's degree in physics from the Naval Postgraduate School, another master's degree in national security strategy; has had a distinguished array of assignments and awards, and they will all be made a part of the record.

We appreciate your service, General Alexander. We appreciate your coming in today. And the floor is yours.

GEN. ALEXANDER: Thank you, Mr. Chairman. Good morning, Mr. Chairman, Senator Leahy and members of the committee.

Sir, I have submitted a formal statement for the record. I'll provide a brief summary of that statement at this time.

SEN. SPECTER: Your full statement will be made a part of the record.

GEN. ALEXANDER: Thank you, sir.

I am pleased to be here today to provide testimony in support of the National Security Surveillance Act of 2006, which would amend the Foreign Intelligence Surveillance Act of 1978. The changes proposed in the bill are, I believe, intended to recapture the original congressional intent of the statute, ensuring the rights of the American people, our original congressional intent, and providing for our nation's security.

As General Hayden indicated in his remarks, this is an important conversation not only for the intelligence community, that will be called on to abide by the statute, but for all the American people.

Advances in technology have had some unanticipated consequences in how the National Security Agency carries out its duties. While some of the specifics that support my testimony and support passage of this bill cannot be discussed in open session, and while I would be happy to elaborate at any time, sir, the full content of that, let me succinctly say that communications technologies has evolved in the 28 years since the bill was established in 1978 into (days ?), as General Hayden says, that were unforeseen by the folks who built that bill.

The stunning technological changes in the communications environment that we have witnessed since the enactment of FISA have brought within the scope of the statute communications that we believe the 1978 Congress did not intend to be covered.

A tremendous communications infrastructure has emerged in the United States. And both our own citizens and foreign persons outside the country use its awesome capabilities. The drafters of the FISA did not and could not have expected to anticipate this. The result, though, as General Hayden's testimony suggested, is that the U.S. government is often required by the terms of the statute to obtain a court order to conduct surveillance of a target of a foreign individual operating overseas but using that infrastructure.

We believe the United States should be able to acquire communications of foreign intelligence targets overseas without a court order and that it ought not to matter whether we do so from the United States or elsewhere or how a particular communication makes its way from point A to point B.

But because of the way the statute defines electronic surveillance, we frequently fail to make the most of one of the greatest advantages we have over our foreign adversaries -- ready access to their communications present on a vast communications infrastructure located in our own nation.

We believe that the FISA of the future must contain a few critical provisions if the government is to be successful in gathering intelligence about its adversaries.

First, the statute needs to be technology-neutral. Determinations about whether a court order is required should be based on considerations about the target of the surveillance rather than the particular means of communication or the location from which the surveillance is being conducted.

Second, we must retain a means to compel communications companies to provide properly authorized assistance to the government, and we must insulate those companies from liability when they do so.

Third, the statute's definition of "agent of a foreign power" should be sufficiently broad to include visitors to the United States who may possess foreign intelligence information, even though they are not working on behalf of any foreign government. The Senate bill that we are looking at would effect the required changes.

In closing, let me again express my thanks to the entire committee for taking up this difficult but crucial issue -- balancing the security of this country and the civil liberties of our people. And thank you for allowing those of us who will implement that balance the opportunity to participate in this hearing.

SEN. SPECTER: Thank you very much, General Alexander.

We now turn to Steven Bradbury, acting assistant attorney general, Office of Legal Counsel. He had been the principal deputy assistant attorney general of the same department. Bachelor's degree from Stanford. A law degree from Michigan, magna cume laude. Has had a distinguished career in the private practice and was a law clerk to Judge Buckley of the D.C. Court of Appeals.

At the outset, Mr. Bradbury, I want to publicly acknowledge your legal abilities and your courtesies in working through the drafting of the legislation which we are considering today, jointly with Michael O'Neill, the chief counsel and staff director of the Judiciary Committee. We're pleased to have you here today, and we look forward to your testimony.

MR. BRADBURY: Thank you, Mr. Chairman. It's been a pleasure to work with you and Mr. O'Neill. And it's a pleasure to be back before the committee today.

Mr. Chairman, Senator Leahy, Senator Kennedy, members of the committee, foreign intelligence surveillance is a critical tool in our common effort to prevent another catastrophic attack on the United States. The enemies we face operate in obscurity through secret cells that communicate globally while plotting to carry out surprise attacks from within our communities.

We all recognize the fundamental challenge the war on terror presents to a free society: to detect and prevent the next 9/11, while steadfastly safeguarding the liberties we cherish. Maintaining the constitutional balance between security and liberty must be the pole star in any legislative effort to reframe the FISA statute.

The past 28 years since the enactment of FISA have seen perhaps the greatest transformation in modes of communication in the history of the world. Innovations in communications technology have fundamentally transformed how our enemies communicate and, therefore, how they plot and plan their next attacks. It is more than a little ironic that al Qaeda is so expert in exploiting the communications tools of the Internet Age to advance extremist goals of intolerance and tyranny that are more suited to the 12th century than the 21st.

Meanwhile, the United States confronts the threat of al Qaeda with a legal regime geared more toward traditional case-by-case investigations. The limitations of the traditional FISA process and the acute need to establish an early warning system to detect and prevent further al Qaeda attacks in the wake of 9/11 led the president to authorize the terrorist surveillance program.

As he has described, that program, which has been the subject of prior hearings before this committee, involves the NSA's monitoring of international communications into and out of the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

This committee is currently considering several pieces of legislation addressing FISA and the terrorist surveillance program. I want to thank the chairman again for his leadership on these issues and for his hard work in crafting a comprehensive approach that will help us fight terrorists more effectively and gather critical foreign intelligence more efficiently.

I also wish to thank Senator DeWine, who has also introduced a bill cosponsored by Senator Graham, which represents a very positive approach to the issues presented by the terrorist surveillance program.

The administration urges the committee to approve both of these bills promptly and we look forward to working with the Congress as a whole as this legislation moves ahead. And with the intel committees, in particular, where technical changes can be appropriately discussed to ensure that FISA, as amended, will provide the nation with the tools it needs to confront our adversaries.

Fundamentally, Chairman Specter's legislation recognizes that in times of national emergency and armed conflict involving and an exigent terrorist threat, the president may need to act with agility and dispatch to protect the country by putting in place a program of surveillance targeted at the terrorists and designed to detect and prevent the next attack.

At the same time, however, Chairman Specter's legislation will provide an important new role for the judicial branch in the review of such presidential programs. In addition to oversight by the intelligence committees of the Congress, his bill would add a new title to FISA, under which the FISA Court, subject to certain requirements, would have jurisdiction to issue an order approving a program of terrorist surveillance authorized by the president. This legislation would create for the first time an innovative procedure whereby the attorney general will be able to bring such a surveillance program promptly to the FISA Court for a judicial determination that it is constitutional and reasonable in compliance with the requirements of the Fourth Amendment.

The FISA Court would also be authorized to review the particulars of the program and the minimization procedures in place to help ensure that the surveillance is focused on the terrorist threat and that information collected about U.S. persons is properly minimized. The availability of these procedures, and the ability of the FISA Court to issue an order approving a program of electronic surveillance, will strongly encourage presidents in the future to bring such programs under judicial supervision.

As Chairman Specter has announced, in response to this proposal and the other positive innovations contained in the chairman's bill, the president has pledged to the chairman that he will submit his terrorist surveillance program to the FISA Court for approval if the chairman's legislation were enacted in its current form or with further amendments sought by the administration.

Chairman Specter's legislation would also protect sensitive national security programs from the risk of disclosure and uneven treatment in the various district courts where litigation may be brought. Under his bill, the United States, acting through the attorney general, could require that litigation matters putting in issue the legality of alleged communications intelligence activities of the United States, be transferred to the FISA court of review, subject to the preservation of all litigation privileges. The court of review would have jurisdiction to make authoritative rulings as to standing and legality under procedures that would ensure protection of sensitive national security information and promote uniformity in the law.

In addition to the innovations I have described, Chairman Specter's legislation includes several important reforms to update FISA for the 21st century. These changes are designed to account for the fundamental changes in technology that have occurred since FISA's enactment in 1978 and to make FISA more effective and more useful in addressing the foreign intelligence needs of the United States and protecting the nation from the unique threats of international terrorism.

Mr. Chairman, thank you for the opportunity to appear today to discuss this important issue. We look forward to working with Congress on this critical matter. And today we urge the committee to give speedy approval to the bills introduced by Chairman Specter and Senator DeWine. Thank you.

SEN. SPECTER: Thank you very much, Mr. Bradbury.

After consultation with Senator Leahy, we're going to set rounds of seven minutes for members and we'll proceed to that now.

General Alexander, there would be much more comfort by everyone, including myself, if we could have individualized warrants so that the FISA Court would function as it does now: an application is made, there's a showing of what the government contends is probably cause and there's an individualized determination on granting the warrant.

Now it has been reported that the program in operation is so massive that that cannot be accommodated. If any of this requires going into closed session, gentlemen, we're prepared to do that. But to the extent you can comment publicly, I think there is great merit in it so that there is an understanding of the program to a maximum extent consistent with national security.

So my question to you, General Alexander: Would it be possible with additional resources to structure a program, to get what information you have, are getting here, on an individualized basis?

MR. ALEXANDER: Sir, let me answer that this way -- and I would ask Steve to make sure I say it exactly correct -- but as General Hayden, Steve and I have laid out for you, if you take away the foreign portion of that, where the (true ?) bill asks us to get a warrant on a U.S. person in the United States, if you take out foreign, overseas, other targets that we're talking about, which your bill does do, you're now back to a manageable level. And getting a court order for everyone in the United States is doable and one that we think should be done in that regard. And it's in the statute.

So the real issue is, intermixed into the domestic is the foreign. Your bill separates that and makes it manageable.

SEN. SPECTER: Let me focus the question more pointedly in light of what you just said.

Is it possible to have individualized warrants where your focus is on a foreign speaker, but your invasion, necessarily, involves a citizen in the United States? Would it be practical to have individualized warrants and still carry out the program which you have now?

MR. ALEXANDER: There is the technology part of the thing that we each discussed briefly, which would --

MS. : (Off mike.)

MR. ALEXANDER: Yes, ma'am.

This is the part that we each discussed briefly in that if overseas we're collecting, going after a foreign target, no matter who that person is talking to, we are authorized under executive order to collect that communications. That's the "where." If we collect it here and it happens to go to a U.S. person, we have to stop and get a court order. So the predominate number of our targets are foreign targets. And the question is, if we make every foreign application, because we're using the infrastructure in the United States, an application that we have to do here in the United States, you have cut out the most important advantage that we have -- our communications infrastructure. That's it.

SEN. SPECTER: General Hayden, let me move to another question with you.

You said that there has been some help/assistance in not having another attack on our soil.

One of the key factors is, in evaluating the intrusion on privacy, how valuable is the information which is obtained? Can you amplify in open sessions whether information obtained has prevented another attack, or to what extent has that information been of significant value for national security in weighing the balancing act of invasion of privacy?

MR. HAYDEN: Yes, sir, Senator. In open session I'll have to speak in generalities, but I can see with great confidence in all three positions, CIA, DNI and particularly NSA, in broad terms the support we get from the broader community of America in all its shapes and forms has been absolutely invaluable in helping, in this case, NSA do its mission.

SEN. SPECTER: Can you say whether it has ever prevented another attack?

MR. HAYDEN: I can say that the program that we're talking about here, the terrorist surveillance program, has been used to disrupt and degrade enemy activity, to break up cells. Can I claim that, you know, there was a sniper on the roof with a (run ?) in the chamber and we intercepted at that point? No. But we've gotten information we would not otherwise have had and it has enabled us to disrupt, clear al Qaeda attempts to do harm inside the United States.

SEN. SPECTER: General Hayden, moving to another issue: When you have the information going to the FISA Court with its secrecy provisions, contrast that with going, say, to a district court, say, in San Francisco. With respect to the complexity of the issues, is the explanation of the nature of the program -- and I'm open to having other courts besides the FISA court. I'm not in concrete on that. In order to get the president's signature to a modified bill we have to have his agreement. But would we have the negotiations? We talked about changes to the bill. The president wants some improvements in the bill. They'd have to be negotiated to his satisfaction. And in wrestling with this issue of consolidation in the FISA Court, we have done so because we know that the FISA Court has a background in the program, has an understanding of the national security risks, knows the details of the program. And we're considering whether it ought to be in other courts. There's an advantage in having other judges and not necessarily having it in a secret court. We have to work through the question as to a public disclosure. When we had an opinion of the FISA appellate court, it was made public, and I think the decision with the FISA Court would reach the public one way or another. But contrast, if you will -- and my red light is not quite on yet -- contrast, if you will, we're taking the cases to a district court like San Francisco contrasted with the FISA Court.

MR. HAYDEN: Mr. Chairman, I'm personally delighted that these issues would be placed in front of a court that, number one, is most knowledgeable about this whole universe of activity and understands, I think in very clear terms, what NSA does as a matter of routine and understands the care with which the agency guards privacy and can make an accurate assessment of the issue that is placed in front of the court. And I would then add that having it in front of a single court, I think actually helps the cause of justice so that there is a unitary national view as to what constitutes the correct balance, the correct line, as Steve has mentioned earlier, between security and liberty.

SEN. SPECTER: Senator Leahy.

SEN. LEAHY: Thank you, Mr. Chairman.

General Alexander, in my opening statement I mentioned that FISA has been amended six times in the last five years. Now to my knowledge, the administration never in that time asked for any of the changes that are contained in Section 9 of the chairman's bill. To the contrary, the administration has repeatedly said that the 2001 Patriot Act updated, modernized FISA. So if Section 9's provisions were so essential, why didn't we hear about them before now? Why this sudden demand for an overhaul of FISA?

MR. ALEXANDER: Sir, I don't know the exact answer for why it was never brought forward, but I can tell you there was great concern about revealing to an adversary an advantage that we had by making public some of the things that we could do. That has happened in the press.

SEN. LEAHY: Well, let me follow that a little bit.

MR. ALEXANDER: Okay, sir.

SEN. LEAHY: I'm told that these -- this request originated at NSA. Is that correct?

MR. ALEXANDER: Yes, sir.

SEN. LEAHY: So, and I'll ask this of you, General Alexander and then General Hayden. Earlier this year the administration did not ask Congress to authorize the so-called terrorist surveillance program, according to what you started to say, because talking about it may tip off our enemy. You think our discussion today about possible amendments to FISA is doing that? MR. ALEXANDER: I don't believe the amendments that have gone in the past have gone to the extent that we're talking about in this change of this bill here. Specifically, we have never brought forward the specifics on the advantage that we have in our home communications Ã,Â-

SEN. LEAHY: Do you believe this discussion is tipping off our enemies in any way?

MR. ALEXANDER: We have to be concerned, sir. Clearly, we do not want to give any advantage to our adversaries. And so the hesitancy is not just my own ignorance on this but making sure that I don't say something --

SEN. LEAHY: General Hayden?

MR. HAYDEN: Yes, sir. When the program began, the terror surveillance program, we at NSA felt we had two lawful approaches in which to conduct our operations against al Qaeda.

One is outlined in the tradition FISA act, the one under the president's authorization. We were quite happy to use both authorities, and we did. And in discussions as to whether or not we should move what had been authorized by the president under both his constitutional authorities and the administration's reading of the AUMF, in the discussions of whether or not we should move that under the FISA act, it really was a compelling concern as to how much of this could be discussed in open session.

What's happened in the last seven months is much of this program has already been put out into the public domain. That inoculates some of the discussion we're having today against some of the downside. But Senator, there will be questions I am sure you will ask any of the three of us that we will not be able to answer in open session.

SEN. LEAHY: Oh, yeah.

Let me ask Mr. Bradbury: When he testified last week, Attorney General Gonzales agreed with Senator Specter that the language in his bill that repeals FISA's exclusivity provision and recognizes the president's inherent authority to collect foreign intelligence is essentially meaningless. To quote the attorney general, quote, "It does not change the status quo." If that's the case, I assume you'd have no objection to striking this language in the bill, if all it does is state the status quo?

MR. BRADBURY: Well --

SEN. LEAHY: Yes or no.

MR. BRADBURY: I'm not able to answer that yes or no, Senator. I will say this: In our approach to these issues, and I think it's reflected in the legal analysis presented in our paper back in January on this program, it's always been our approach to endeavor to avoid a constitutional clash between the branches. And we think that's the way a court would address these issues.

SEN. LEAHY: But the attorney general said -- do you agree with the attorney general when he says all this does is state the status quo?

MR. BRADBURY: Well, the status quo certainly is the case, Senator, that the president has authority under Article II -- SEN. LEAHY: Do you agree with the attorney general?

MR. BRADBURY: -- and the status quo is as the court of review --

SEN. LEAHY: (Inaudible.)

SEN. SPECTER: Let him finish his answer.

SEN. LEAHY: But he's not answering my question.

SEN. SPECTER: Well, let him answer.

SEN. LEAHY: Do you agree with the attorney general?

MR. BRADBURY: I agree that as the court of review, the FISA court of review has stated, that the FISA statute cannot take away the president's constitutional authority.

SEN. LEAHY: Okay. So -- so I don't know whether you agree with the attorney general or not. I'll let you discuss it with him, whether you agree with him or not.

Suppose the government wants to monitor telephone conversations, e-mails coming into the United States from American soldiers serving in Iraq. Now, let's stipulate it does not apply, this is not being done -- this is for you, Mr. Bradbury -- is not being done for law enforcement purposes, so Title 3 doesn't apply. Now, under current law, if the government acquired these communications off wires in the United States, it would need a warrant. What about the new definition of electronic surveillance in the chairman's bill? Would the government still need a warrant to intercept communications from our men and women in Iraq to their family members back at home?

MR. BRADBURY: If you're talking about a communication which is international, and if you're not targeting a person in the United States to try to collect information about that person in the United States, it would not fall within the amended definition of electronic surveillance.

SEN. LEAHY: So you would not need a warrant to collect it? They're e-mailing to their parents, spouses, whatnot, back home. You wouldn't need a --

MR. BRADBURY: If you're attempting to collect information about persons in the United States, which you -- it depends --

SEN. LEAHY: No, no, no, no. I left out that -- I said, there is no law enforcement in it, it is simply --

MR. BRADBURY: Well, Senator, it doesn't have to be law enforcement. Any effort to collect information about persons in the United States would fall within the definition of electronic surveillance, if you're targeting those persons. So you really need to look at -- and that's, I think, the fundamental point that the generals have made, is what we believe the statute ought to focus on is who is it you're trying to collect information about and --

SEN. LEAHY: I made it very clear. I said do you have a soldier in Iraq -- let's make it even clearer. A soldier in Iraq is sending an e-mail to his wife. You're not looking for law enforcement, he's not suspected of doing any crime or anything else. Would you need a warrant to collect that e-mail, or could you just pick it up and put it into your government banks?

MR. BRADBURY: Well, I will say, Senator, that today, under existing law, if you are collecting that internationally flowing communication, anywhere else in the world you can do that without any court approval. That's done today, pursuant to executive order when it's done for national security purposes. Now, these agencies operate for national security purposes and not simply to eavesdrop on people's private conversations when there isn't any national security interest or foreign intelligence --

SEN. LEAHY: Would your message be then that somebody sending an e-mail to their spouse back here from Iraq, they'd probably better be pretty careful what they say, that it's going to be in government database somewhere? MR. BRADBURY: No, I wouldn't, because as I've tried to just indicate, all of the authorities of these agencies, when they're operating today, Senator, under executive order -- it's called Executive Order 12-333, which we've existed under since the 1970s -- the only collection that these agencies can do under that executive order is for foreign intelligence purposes. That's quite apart from any statutory requirements under FISA. So there's no listening in, except for foreign intelligence purposes, and that's the fundamental point. It doesn't matter whose communication you're listening in to, or where it's collected. It has to be for foreign intelligence purposes.

SEN. LEAHY: Doesn't answer the question, but I'll go to my next --

SEN. SPECTER: The vote is under way. We're going to adjourn very briefly. Senator Cornyn and I are going to be very swift in moving over and back, and when we come back, we'll pick up with Senator Cornyn.

We stand in recess for just a few minutes. (Raps gavel.)

RECESS

SEN. SPECTER: The committee will resume.

Senator Cornyn.

SEN. JOHN CORNYN (R-TX): Thank you, Mr. Chairman.

And I want to express my gratitude to the witnesses for being here today to talk about this important subject. I would hope that we could all start from a basic premise, and that is that we should use all legal means available to us to collect information from our enemies that would help us fight and win the global war on terror.

I think that we would all agree with that. I'm confident you would. Sometimes I wonder, when I hear some of the public debate.

But I want to maybe start with you, Mr. Bradbury. You know, early on, when The New York Times broke the story about the terrorist surveillance program, there were allegations that there had been a violation of the law, that this is unlawful.

But as the chairman pointed out, my recollection is there have been at least three courts that have expressly acknowledged the president's inherent power under the Constitution to collect foreign intelligence during a time of war. Is my recollection correct?

MR. BRADBURY: That's correct, Senator. The 4th Circuit, the 2nd Circuit, other circuits -- in fact, more than three -- and then, of course, the FISA Court of Review acknowledged that.

SEN. CORNYN: Well, that was going to be my next point, that the very court that Congress created to oversee the decisions of the Foreign Intelligence Surveillance Court, the FISA Court of Review, has acknowledged in a written opinion the president's inherent authority under Article II to conduct this, in essence, battlefield intelligence-gathering. Isn't that right?

MR. BRADBURY: That's correct, Senator.

SEN. CORNYN: Are you aware of any court that has held the Terrorist Surveillance Program to be unlawful?

MR. BRADBURY: No, Senator. No court has reached that issue. SEN. CORNYN: So the only courts that have spoken to it have held that this is a lawful exercise of the president's authority under the Constitution.

MR. BRADBURY: The only decisions from courts are that the president generally has authority, under Article II, to protect the country through foreign intelligence surveillance.

SEN. CORNYN: Well, I would hope that because -- I agree with your assessment; that's certainly my understanding. And I would hope that those who would try to scare people or make allegations of rampant sort of unlawful or rogue conduct would bring their rhetoric down a little bit, because, in fact, the only decisions we do have from courts indicate that the president does have that authority under appropriate circumstances.

I want to also ask, General Hayden and General Alexander, there was some statement made early on in the hearing today that the capability that the NSA has been using, that the United States government has been using to intercept international communications between al Qaeda operatives and folks here in the United States who may be their allies, that this is somehow unchecked authority.

But I just want to ask a little bit about that. It's my recollection that this program is reviewed every 45 days internally within the NSA and the administration. It's my recollection that it's been briefed to the FISA Court judges, if not all of them, at least the chief judge, and maybe some others; if you can help me there.

It's also been briefed since the inception to leaders, on a bicameral and a bipartisan basis, the leaders of the House and the Senate, as well as the chairman and ranking members of both the House and Senate Intelligence Committees. Did I summarize that correctly?

MR. HAYDEN: Yes, sir. That's correct, Senator.

SEN. CORNYN: Well, to me, that seems like it comes in some conflict with the idea that this authority is unchecked. And that's my conclusion. You don't have to agree or disagree.

And one reason I support Senator Specter's bill is because it does acknowledge this authority, but it creates a way to try to accommodate the legitimate concerns that members of Congress have and to make sure that Congress is a full partner in the process of striking the balance that, General Hayden, you talked about between privacy concerns and our ability to collect intelligence by all lawful means.

Mr. Bradbury, I wonder, though, if you could tell me, do you view this bill to be a substantial change from the status quo? There was some question about that. Or is it a ratification, more or less, by Congress that the president has that authority and then create other procedures that are essentially consistent with what's already happening now?

MR. BRADBURY: Well, of course, Senator, as the chairman made clear in his opening remarks, the status quo today is that the president has exercised his authority, both under the Constitution and his view of the authorization for the use of force, and has established the Terrorist Surveillance Program, independent of FISA, in an effort to try to detect communications that may be leading to another attack on the country.

And so this legislation would make -- would recognize that existing fact, but it would make a very substantial change in FISA today by adding a new title that would give the court jurisdiction to review such a program on a program-wide basis.

And that is an important new tool that any president would have going forward. And it's because of that innovative new tool that would really allow for efficient judicial review of such a program in wartime that the president would take the program then to the court for its review.

So I applaud, again, the chairman for the legislation and for that effort, because I do think that's very important -- would be a very important change in the current statutes.

SEN. CORNYN: Well, thank you very much for that clarification. And I think you're certainly correct. I know, General Alexander, there was some question about whether the NSA was intercepting Internet communications between a soldier in Iraq and their family members at home. You're a soldier, are you not, sir?

MR. ALEXANDER: Yes, sir.

SEN. CORNYN: And you certainly, I know, have an interest in not undermining the privacy rights of an American citizen serving his country and defending freedom in Iraq. Do you -- are you spending your time targeting American citizens, soldiers in Iraq, just in your spare time?

MR. ALEXANDER: No, sir, we aren't, nor would we. If we do, we have procedures through the attorney general overseas, if it's against a U.S. person, or a court order here in the United States. And both of those would be followed.

I will tell you, I would be more concerned about other nations looking at our soldiers, which they do, than terrorists. And so the fact that we can do it, others can do it too. And so the greatest concern is the operational security that goes along with soldier communications, which they in Iraq know very well. And as you know, sir, from the soldiers there, they treat OPSEC like it's very important to their own survival.

MR. HAYDEN: Senator, if I can just emphasize a point that General Alexander brought up, the procedures in place today, which will not be affected by the act before the committee, is that in order to target a protected person, a U.S. person -- and that definition goes beyond just citizens of the United States -- in order to target a protected person overseas now requires, well, now General Alexander to make a case to the attorney general that this is for foreign intelligence purposes and that the target of the activity is the agent of a foreign power. And that would not be changed by the legislation.

MR. BRADBURY: I'm sorry, just to emphasize that triply, what I mentioned before in response to the question from Senator Leahy is that there are authorities today under executive order to do foreign intelligence surveillance. But those authorities, if you're talking about targeting the communications of a U.S. person, like a U.S. soldier in Iraq, require both that it be for a foreign intelligence purpose and that the attorney general expressly approve it. And that's under existing executive order. That would remain unchanged by this legislation.

SEN. SPECTER: Thank you, Senator Cornyn.

Senator Kennedy.

SEN. KENNEDY: Thank you very much.

And I want to thank the panel, thank them for their service to the country -- impressive backgrounds and experience and commitment. I was here when we did the FISA legislation; at that time, in '76, President Ford and Attorney General Levi. And they worked very closely with the Judiciary Committee, the president and the attorney general, and we worked out the FISA.

It was enormously complex and complicated at that time, and the range of intelligence challenges are like an echo that I hear this morning. Everyone understood that there was cutting edge; it was new information, dangerous time. And we were able to work out legislation that only had one vote in opposition to it in the United States Senate, and it has worked.

Obviously there are suggestions and recommendations that can be made, but it worked and it had the confidence of the American people and the confidence of the Congress about the protections of rights and liberties, and also in getting information.

All of us are in the same boat in terms of al Qaeda and the dangers that are before this country, but as you have all eloquently stated, the balance between the security and also the liberties that we have to deal with. And that is what many of us had hoped, that we would be able to work with an administration -- would work with us.

We can handle the sensitive and secret information and establish a process that I think would have given the American people the confidence that all of us were working together, Republican and Democrat, the president and the Congress, bipartisan way, to really get at the core dangers that we face in protecting liberties. And that is what I think continues the challenge. And the fact that we are still working on this is just enormously important.

But that's the departure point, and it still continues to be frustration that we were unable to get to that point and don't have all of the information that we should have in order to legislate. The American Bar Association points out the challenges that we're continuing to face under the circumstances.

I'm interested, in the time that I have, if you can just tell us -- and we're very conscious of the fact that there's sensitive information on this -- but can you tell us now the extent that this is actually affecting the Americans, Americans here at home? What are we talking about, to the extent that they are included in this program?

MR. HAYDEN: Senator, I'll start --

SEN. KENNEDY: Okay.

MR. HAYDEN: -- since I was there when the program began. I mean this very sincerely -- nothing more important to the people conducting this program than the privacy of Americans.

SEN. KENNEDY: Good.

MR. HAYDEN: We understand nothing more important in the conduct of this program than the privacy of Americans.

After the story broke in The New York Times, I went out to talk to the NSA work force that is involved in this, and it struck me that on the walls of the office in which this activity is conducted, there was a large poster that said, "What constitutes a U.S. person?" And the four different approaches by which one could gain the protection of a U.S. person were spelled out there, even in the bowels of the office that is responsible for this program.

It is done very carefully. It is very targeted. There is a probable-cause standard before any communication is intercepted that one or both communicants is, again, through a probable-cause standard, associated with al Qaeda. So I know the sensitivities, Senator. NSA is a powerful and a secretive organization. Those are the two things our political culture distrusts the most. But this is done with great care.

SEN. KENNEDY: Well, I understand that. And the standard, then, is the probable-cause standard. Is that correct?

MR. HAYDEN: That's correct.

SEN. KENNEDY: All right. But the question was to the extent the number of Americans that are included in this. Can you tell us, or is that -- what is the extent? What is the range?

MR. HAYDEN: We have briefed the precise numbers to all members and some numbers of staff to both Intelligence Committees, Senator.

SEN. KENNEDY: But even in the range -- if you can't, you can't. But, I mean, are we talking about 20,000? Are we talking 2 million? Can you -- you can't do it in that --

MR. HAYDEN: I'm not able to.

SEN. KENNEDY: All right. Can you tell us whether any of these are continuing surveillance; that is, that they go on for not only just a conversation but whether they are continuing, whether there are Americans that are subject to continuing -- this was an issue when we passed the FISA. Attorney General Levy spoke about this issue and question in terms of the legality of it. And this is an area that obviously is of concern. Can you tell us?

MR. ALEXANDER: Sir, if I can give you two things here in open session. The overwhelming focus in our collection is against the foreign entities, by a tremendous margin. And everyone who has read into that is amazed when they see that, first and foremost, predominantly foreign.

There are U.S. parts to that. And I can't go into the details of the lengths of that, but it is all focused on the al Qaeda and it's predominantly -- go ahead, sir.

MR. HAYDEN: I'd just offer a point to make it very clear. The president has said the communication we believe to be affiliated with al Qaeda, associated with al Qaeda, one end of which is in the United States, and we believe at least one end we have a probable-cause standard is al Qaeda. As General Alexander points out, overwhelmingly the end we believe to be affiliated with al Qaeda is a foreign end.

SEN. KENNEDY: All right. And so just about the question about it continuing and ongoing versus a conversation, the extent of that, General Keith -- Alexander?

MR. ALEXANDER: Sir, I'm not sure I understand.

SEN. KENNEDY: One thing is whether you're listening to a conversation; the other is whether you have the wiretap that is continuing 24 hours a day.

MR. ALEXANDER: Right. Sir, we go through a very deliberate process to listen in on any conversation, just because of the sheer resources, whether it is in this program or any other program.

And so as we started out, we know it's one end foreign -- you cannot physically listen to millions of phone calls, nor would we.

SEN. KENNEDY: Okay.

MR. ALEXANDER: We are going to focus it down onto the most important ones, and we have ways and methods to do that that I would -- that we could -- should not discuss here.

SEN. KENNEDY: All right. I'm going to run out of time here. But let me ask you: Has any of the information been -- that has been gathered to date in any of this been used in any legal proceedings here, in any courts or any trials to date?

MR. ALEXANDER: Senator, the process used is the process by which we use any foreign intelligence, and it is -- it moves outside of the intelligence community with all the appropriate caveats on it, in terms of how it can be used in judicial procedures.

SEN. KENNEDY: But can you tell us whether it has been or hasn't been -- been used?

MR. : I don't know.

MR. : I don't know.

MR. ALEXANDER: I don't know, Senator, because -- again, because we put the caveats on it --

MR. : It's for lead and investigative --

MR. ALEXANDER: -- for lead and investigative purposes of what it says.

SEN. KENNEDY: Time is up, Mr. Chairman. Thank you.

SEN. SPECTER: Thank you, Senator Kennedy.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman, and thank you for the hearing.

I'd like to just say one thing, and that is, as a member of the Intelligence Committee, I have been briefed on the program. And I am strongly opposed to giving this president or any president the right to collect content, to collect content on United States persons without a warrant.

And today, for the first time, we heard General Alexander state that if the foreign-to-foreign switching is taken care of, that the program is easily accommodatable to an individual warrant for U.S. persons in content collection. Is that not correct, General?

MR. ALEXANDER: Not quite, ma'am. If I might just state in my words, that if the foreign selectors that we're going after, which -- some of those -- depends on where the target is -- and this goes back to the definition of electronic surveillance. And so it's not necessary -- if we're going after a terrorist in Country A, and he's talking to somebody in Country B, we're authorized to go after that.

If that same terrorist we're targeting happens to go into the United States, we're authorized to collect that overseas also and minimize the U.S. person's data.

The issue that I was describing is, now, under the current FISA, if I collect that in the United States, I have to get a warrant for it. So what you would have us do is -- overseas I could do it and minimize it. Today I lose the advantage of being able to do that in the United States. If that portion of the targeting -- in the definition of this electronic surveillance -- we believe that is adjusted in this proposal, that meets both of those, and that that would then allow us to --

SEN. FEINSTEIN: And both ends are foreign-to-foreign?

MR. ALEXANDER: Not necessarily. The target of the selector is foreign. And the question is, where are they calling? But we don't --

SEN. FEINSTEIN: Well, I know those numbers, too.

MR. ALEXANDER: Right.

SEN. FEINSTEIN: And I do not think that those numbers are necessarily prohibitive from a FISA warrant, nor do I believe that it would take that much time for a FISA warrant.

MR. ALEXANDER: But it would require us, ma'am -- if I might, it would require us to get a FISA on every foreign one in advance, because we don't know who they're calling until it's happened.

SEN. FEINSTEIN (?): Oh --

MR. BRADBURY: Senator, may I also just add a point, if I might?

SEN. FEINSTEIN: Certainly. MR. BRADBURY: In the chairman's legislation there would also be a number of other reforms to FISA which would greatly assist in the general ability to get FISAs, even for domestic targets. For example, the FISA application process would be streamlined. The amount of information required for an application would be reduced --

SEN. FEINSTEIN: That was in my bill, too.

MR. BRADBURY: -- yes, it was -- and that --

SEN. FEINSTEIN: I believe Senator Specter took it from my --

MR. BRADBURY: Absolutely. It's a good idea -- (laughter) -- and good ideas should be liberally --

SEN. FEINSTEIN: I just wanted to make that clear.

SEN. SPECTER: I had thought that was our bill, the Feinstein- Specter --

(Laughter.)

SEN. FEINSTEIN: (Laughs.) I'm delighted! Yes, it is our bill.

MR. BRADBURY: In addition -- and this may also be in your legislation, Madame Senator -- the emergency authorization period would be extended from three days to seven days. The ability to authorize it would be liberalized. And then, perhaps most importantly, if the reforms are made to the definition of what's covered to take out the international communications that are not really historically the primary focus of FISA, that, of course, by itself would free up a lot of resources in terms of the Office of Intelligence Policy and Review that makes the applications to FISA. So all of those combined would necessarily make it much easier to get quick approvals for those domestic targets of necessary intelligence surveillance.

MR. ALEXANDER (?): And that's why I tried to craft my opening comments about those four criteria. And very frequently, NSA is required to get FISAs not because of who is targeted, but because of one of those other three criteria. And what this legislation does is move the legal focus back to who are you targeting rather than these techniques or accidents of how you actually carry it out.

SEN. FEINSTEIN: Well, let me raise one other point. Senator Specter's new FISA bill also eliminates the 15-day window on surveillance following a declaration of war. And this could be interpreted to mean that after a declaration of war, the president has unlimited wiretap authority till the end of the war. And how long, under the new Specter version, would a president's authority last? Could it last for decades?

MR. BRADBURY: Well, Madame Senator, the president's authority to protect the country comes in large measure from his authority under Article II.

And, of course, with the terrorist surveillance program, that has been in place now since shortly after 9/11.

It is our view, as we tried to explain in --

SEN. FEINSTEIN: If you don't mind, let me just interrupt you.

MR. BRADBURY: Absolutely.

SEN. FEINSTEIN: Because it seems to me you are buying in -- the administration is buying in to a concept, and that's Senator Specter's bill. Therefore, you are tacitly confining your Article II authority within the confines of the Specter bill, as I understand it. So I am asking you the question, one of the amendments made is to delete this 15-day period, which, therefore, once deleted, also has an interpretation that it is without end.

MR. BRADBURY: Well, there would be no express provision that says in time of war that the limitations of FISA do not apply. The current provision says if there were a declaration of war, none of the requirements or limitations in FISA would apply at all for 15 days. Now, there's only been five declarations of war in the history of the country, and we haven't even come close to one since FISA was enacted in 1978.

It's our view of that provision today in the legislation that, in effect, it's a determination by Congress back in 1978, which was not a time of war, that in the event of armed conflict or a declaration of war, that the branches would come together and that there would be some accommodation made going forward in that -- during that wartime. It's not our view that it was a declaration by Congress that only 15 days of warrantless surveillance in wartime is all you need. I don't think that's what it was intended to mean. It was intended to give some leeway -- all the rules are off -- and then during that period, there would be some special accommodation made. It was really, in effect, a decision by Congress in the 1970s to punt the question of what would happen during an actual armed conflict.

SEN. FEINSTEIN: Mr. Chairman, would you allow me one other question?

SEN. SPECTER: Yes, proceed, Senator Feinstein.

SEN. FEINSTEIN: Yeah. Perhaps, Mr. Bradbury, you're the one to ask this question of. Is it your contention that the FISA Court is an Article III court?

MR. BRADBURY: The judges are Article III judges. And, yes, they're serving in a special capacity for purposes of approving these orders, but, yes, they are Article III --

SEN. FEINSTEIN: And to what do you attribute that? I mean, where is the justification for finding it in an Article III court?

MR. BRADBURY: They are appointed for life with their compensation fixed. It can't be reduced. They are Article III judges, and Congress, by statute, has given them a special assignment at the appointment of the chief justice, but that does not mean that they're not Article III judges. They act in their capacities as Article III judges, as does a court that approves, for example, a Title 3 warrant.

SEN. FEINSTEIN: Isn't there a magistrate serving as a FISA Court judge?

MR. BRADBURY: I'm not aware of that. There are 11 FISA Court judges. I believe -- don't hold me to this -- that they're all district judges appointed by the chief justice.

SEN. FEINSTEIN: Well, I'm a little puzzled, Mr. Chairman, on this one point, because there is nothing in the FISA law that gives this court the ability to make programmatic approvals as opposed to grant warrants, individual warrants. And how a court gives an advisory approval to a program and the constitutionality of such, I think, is questionable.

MR. BRADBURY: Well, may I respond to that?

SEN. FEINSTEIN: Yes, please.

MR. BRADBURY: Interestingly enough, the FISA Court of Review, in the In re Sealed Case decision, addressed the question of whether a FISA order under the current statute is a warrant or not. And the court actually concluded that, while it has a lot of characteristics of a warrant, the court did not need to conclude or decide that it was a warrant because foreign intelligence surveillance could be conducted before and after FISA, as long as it's reasonable under the Fourth Amendment, and that the FISA procedures would ensure that any court order approving surveillance would ensure that that surveillance was reasonable under the Fourth Amendment. So there isn't -- it's not necessarily the case that a FISA order, even an individualized one, is a warrant for Fourth Amendment purposes. And the Fourth Amendment does not require a warrant in all circumstances. In special cases, there can be surveillance done, searches conducted without warrants -- as long as they are reasonable -- for example, in the area of foreign intelligence investigations and surveillance.

The -- but you are --

SEN. FEINSTEIN: Are you making the argument that a FISA Court order for content collection is not a warrant?

MR. BRADBURY: Well, the FISA Court of Review concluded that it did not need to decide that it was a warrant for it to be constitutional, so it does not have to be viewed as a warrant.

And I would say that you're right, that today FISA does not contain any procedure that would allow the FISA Court to give a program-wide order of approval to surveillance. The new title that would be created by the chairman's bill would enable the court to do that and would give the court jurisdiction.

But in terms of Article III and whether there's a case or controversy, I don't see a difference between the program-wide order and the individualized order. There would still be a case or controversy, it would be constitutional. The attorney general, as a result of that order, can get an order from the court that would compel cooperation to do what needs to be done to undertake the surveillance. And just as with a Title 3 warrant today, where the government goes in ex parte to a district judge and gets approval for a Title 3 warrant, this is a similar construct, and it's similar to the FISA process today for FISA orders.

There is the hypothetical person on the other side of the case -- not hypothetical, but the people on the other side of the case are those people who would be under surveillance.

That's the same in a Title 3 context or under FISA today. I really think it would function like FISA today; it would just be a program- wide order.

SEN. FEINSTEIN: Well, you've been more than generous with your -- (inaudible) -- Mr. Chairman --

SEN. SPECTER: How much more time would you like, Senator -- how much more time would you like, Senator Feinstein?

SEN. FEINSTEIN: Well, you see, I think this is kind of the crux of the matter, and --

SEN. SPECTER: Senator Feinstein, proceed.

SEN. FEINSTEIN: If you just allow me for a minute. Essentially, there are no holds in your bill on a president's authority. Once there is this programmatic approval by the FISA Court, then individuals in this country can be wiretapped for content, and that wiretapping could go on forever. There is no duration. I would assume that others could be slipped into that program, perhaps even without review. And what worries me is that once for content -- metadata is something else -- but for content, once you go to a programmatic approval, it opens the pandora's box of all kinds of games that can be played with that, because there is no timely periodic review of everybody that -- whose content is being collected under that programmatic review; no decisions made as to how long that data can be maintained; when a decision can be made that the data should -- that the content collection should be cut off.

MR. BRADBURY: Senator, that's not the case. Under the chairman's bill, all of those things would be addressed by the court in its review. So, for example, strict requirements would be, before the court would be able to entertain such an application, it would have to be directed at the foreign terrorist threats. There would have to be a showing that it -- that you couldn't use traditional FISA process. There would have to be a showing that there's special need for agility and flexibility and that you cannot identify all of the targets in advance. Then, there would have to be special minimization procedures proposed and in place to protect any information about U.S. persons that might be caught up in the program.

Then, the court would review it for reasonableness under the Fourth Amendment. The Fourth Amendment is not an open-ended blank check. The Fourth Amendment would not allow things to go on permanently. It would not allow things to be general and not focused on the threat. All of those things would be taken into account and reviewed carefully by the court. It could only be approved for 90 days, and then, the court would review it. You'd have to come back in, and in reviewing it and reauthorizing it, the court is charged under the legislation to look at, "Well, what has the actual collection been? Has it been focused as the attorney general said it would be? Have the minimization procedures been followed?" All of those things would be subject to careful judicial review by the FISA Court.

SEN. FEINSTEIN: All right. Knowing the numbers of the foreign- to-foreign --

SEN. SPECTER: Senator Feinstein -- Senator Feinstein, you're up to eight minutes over, which is another round. Why don't you ask your last question.

SEN. FEINSTEIN: The last one. Knowing the numbers of the foreign-to-foreign, you're saying every one of them would be reviewed every 90 days?

MR. BRADBURY: Well, in the terrorist surveillance program of the president, we're talking about international communications in and out of the United States, and under the chairman's proposal for this new program-wide order, it would be focused on surveillance where the -- where you're talking about communications to or from persons in the United States. So the foreign-to-foreign would not be the subject of such a program-wide order. But communication surveillance where there's a U.S. -- there's somebody in the United States who's involved, could be and would be the subject of such a program, and the court would be free to ask, as the legislation makes clear, for any additional information the court desires to review that program and to take a look at very carefully and closely. So it would be up to the court in making a judgment as to the reasonableness of the program, the targeted nature of it, et cetera.

SEN. FEINSTEIN: Thank you. I appreciate it very much. Thank you.

MR. BRADBURY: Thank you, Senator.

SEN. SPECTER: Thank you. Thank you, Senator Feinstein.

General Alexander, coming back to the question which I asked initially and you've expanded upon, would it be impractical or impossible -- or even impossible to have individualized warrants under the current surveillance program?

You had responded in part that it would limit you when you were going after a foreign number, foreign caller, someone who initiated the call abroad, not knowing whether it was going to be to a domestic location or not. Would you expand upon that?

MR. ALEXANDER: Yes, sir. And I'll take from the testimony that we started out with, in that who and where are the key parts of this. Who is the target that we're going after? Is it a foreign terrorist in a country outside the United States? If the target is outside the country making a call, then we should use every means possible -- and I think everybody generally agrees with that -- to go after that communication. The issue is, if we conduct that in the United States and it happens to stop in the United States, in the United States we'd need a warrant; outside the United States we could do it under executive order. So we have a problem. And the issue then becomes do I get a court order for every foreign target that I have under the possibility that I could have collected it in the United States? That's what it does to us today. That is impractical. It would cause a tremendous burden on --

SEN. SPECTER: Now, specifically, what is impractical? When you start -- wait a minute.

MR. ALEXANDER: The volume. The volume --

SEN. SPECTER: Wait a minute. Let me ask the question so we have the framework.

Is it impossible or impractical to get an individualized warrant when the caller is outside the United States, not knowing whether the recipient will be inside the United States?

MR. ALEXANDER: Yes, sir, it would be impractical. I'm not saying it would be impossible, but it would be impractical because we don't know what the foreign to U.S. number could possibly be. Would the requirement be, hypothetically, if that foreign number called all foreign numbers, you'd say good to go. But if they called U.S. number one -- FISA. If he calls U.S. number two, I have to get a new FISA. U.S. number three, a new FISA. U.S. number four, a new FISA. And what I'm ending up doing is submitting for calls that have been happening, and what we would do is saturate ---

SEN. SPECTER: That's what you have to do, absent the surveillance program? MR. ALEXANDER: That's correct --

SEN. SPECTER: But with the surveillance program, you don't have to do that.

Now, you say impractical, but not impossible.

MR. ALEXANDER: Well, you would not be effective. In my opinion, sir, from an operational perspective --

SEN. SPECTER: Why not -- why not effective?

MR. ALEXANDER: Because you would be so far behind the target, if you were in hot pursuit, with the numbers of applications that you would have to make and the times to make those, you could never catch up to the (target ?).

SEN. SPECTER: So your conclusion is that to have individual warrants, it would not be practical or effective in what you're seeking to accomplish.

MR. ALEXANDER: That's correct.

SEN. SPECTER: General Hayden, I think it would useful if you supplemented your oral testimony in writing, amplifying so you have an opportunity to present a fuller picture. We've had a pretty good dialogue here.

SEN. FEINSTEIN: I might say particularly on --

SEN. SPECTER: Now, are you on your time, Senator Feinstein? Let me -- let me proceed, Senator Feinstein. We'll come back to you after Senator Leahy, if the next vote doesn't come sooner.

Mr. Bradbury, Senator Feinstein said that there are no holds and no limitations on what the president can do under my bill. But isn't it a fact that what the president can do under my bill is what the president is doing now, and that it is measured by whatever his Article II powers are?

MR. BRADBURY: Well, that's certainly correct.

SEN. SPECTER: And isn't the determination as to whether he has Article II powers to do what he is doing now a balancing test so that on this date of the record, this committee, not knowing the details of the program, is not in the position to say that it is an exercise within Article II or it is beyond Article II? Is that true?

MR. BRADBURY: That -- that's true. And I would add that the limitation and the real balancing test comes into the Fourth Amendment, because whatever the president does is subject to the Fourth Amendment --

SEN. SPECTER: But we can't determine that unless we know what the program is. Or on the balancing test, reasonableness, as you said earlier, depends on the threat and depends upon the invasion of privacy.

MR. BRADBURY: That's correct.

SEN. SPECTER: And that requires a judicial determination.

MR. BRADBURY: Well, that's one very effective way to do it. And that's what your legislation would do. It would bring the court in to make that determination.

SEN. SPECTER: Is there any other way to obtain a judicial determination other than the FISA court, maintaining the secrecy that the president insists upon?

MR. BRADBURY: Well, I think that's a very good mechanism for doing that. Obviously, the 30 or so pieces of litigation around the country that have challenged various versions of what has been alleged in the media, we do not think those disparate matters in litigation in various district courts around the country is an -- is an effective or appropriate way for any of these determinations to be made.

SEN. SPECTER: Let me move to a series of questions with the minute I have left. Isn't it true as a practical matter, de facto, that the Foreign Intelligence Surveillance Act is not now the sole means of wiretapping in the United States, where you have one party in the United States and one party out of the United States?

MR. BRADBURY: That's correct. The president's program is outside of FISA. SEN. SPECTER: And isn't -- and isn't it -- isn't it so -- FAST is not the exclusive way. And isn't it also true that no statute, including the one I propose, can expand or contract the president's Article II powers?

MR. BRADBURY: Well, I would say that statutes can reasonably regulate exercises of the president's constitutional authority, but where we see a real issue -- and it's a very significant constitutional issue, and that's what the FISA Court of Review is talking about, is an effort to try to eliminate it or snuff it out. And that's where you get a real direct clash between the branches. And that's what we've always endeavored to avoid throughout this discussion. And I think your legislation recognizes that we all want to avoid that particular --

SEN. SPECTER: With Senator Leahy's acquiescence, I'm going to pursue this just a bit further. When you talk about reasonably regulated and you come to Justice Jackson's famous concurrence in the steel seizure case, he said that when the president exercises his constitutional power plus a grant of authority from the Congress under Article I, then his power is at a maximum, because he has two powers: Article II and Article I.

MR. BRADBURY: That's correct. That's correct.

SEN. SPECTER: Where he exercises his Article II power alone, it is at the medium point. Where he faces a situation where Congress has denied him certain authority, as where FISA is in existence, then he relies solely on his Article II power. But isn't that Article II power whatever it is as determined by the balancing test on the invasion of privacy versus the national security interest involved?

MR. BRADBURY: That's right.

SEN. SPECTER: Final -- final question. This -- this provision in the bill has been cited repeatedly as a negative comment: "Nothing in this act shall be construed to limit the constitutional authority of the president to collect intelligence with respect to foreign powers and agents of foreign powers," close quote.

Now, the best illustration of that is a wiretap of a foreign embassy.

Isn't it true that that line was in the FISA Act of 1978?

MR. BRADBURY: It was. I believe, Mr. Chairman, it was amended to take it out at a later point, and this legislation would reinstate it in the bill. But I think the important point is that the FISA Court of Review in its decision says essentially just exactly that, and this is simply a recognition or affirmation of what the FISA Court of Review has said. You're -- in pointing to the embassy provision, you're exactly right; that that's an example where FISA today recognizes and allows for the executive branch to take action without a court order to undertake foreign intelligence surveillance. And that's an authority that exists today and that is recognized in the FISA statute.

SEN. SPECTER: So in totality, Article II power is what it is, and it can't be added to or subtracted by legislation since the Constitution supersedes legislation?

MR. BRADBURY: The legislation doesn't change Article II authority. It can add Congress's authority, as Justice Jackson indicated in his concurrence, or it can attempt to leave the Article II authority as it is, or it can attempt to take away from it whatever Congress -- whatever authority Congress would otherwise provide. And --

SEN. SPECTER: But Congress doesn't have any authority by statute to change the Constitution?

MR. BRADBURY: That is correct.

SEN. SPECTER: Including Article II?

MR. BRADBURY: That is correct.

SEN. SPECTER: Senator Leahy, you have at least 10 minutes or longer.

SEN. LEAHY: Thank you.

Of course, we don't amend the statute by -- amend the Constitution by statute. But as Youngstown pointed out, there are many areas where the president's Article II powers are circumscribed by statute. Is that not correct? MR. BRADBURY: Yes, in the exercise of those authorities, but not where those authorities --

SEN. LEAHY: Thank you. I was glad to get a simple declaratory judgment -- (light laughter) -- a simple declaratory answer from someone from the Justice Department. It's been years! I compliment you, Mr. Bradbury. I compliment you. You'll probably get fired for doing that, but I compliment you for doing it.

But the language that Senator Specter quoted was -- that you never enacted; it was struck from the conference in 1978, as I recall -- but there are areas where we can -- the Congress, under Article I, can determine the actions of the president under Article II. And then, the president, of course, has -- in his oath of office, he says that he will faithfully execute the laws of the United States. Now, of course, if he doesn't like the laws, he can always veto them.

But General Alexander, let's go back to the Terrorist Surveillance Program because we may have been discussing two things in your answers to the earlier questions.

Let's say that under this program you established probable cause; a particular individual you're monitoring is a terrorist and those individuals within the boundaries of the United States.

At that point, do you go to FISA for a warrant?

MR. ALEXANDER: Not necessarily, sir.

SEN. LEAHY: I know --

MR. ALEXANDER: Maybe. Maybe. It would definitely go to one of the other Intel agencies as soon as that is. Our objective would be -- NSA would not be -- would not proceed at that point. We would pass it to either the FBI --

SEN. LEAHY: You're going to continue -- you've got somebody in the United States.

You've established probable cause. And this is prescinding for the moment whether the original program is actually authorized under the law or not. But let us assume you've got probable cause that somebody in Middlesex, Vermont, is a terrorist. I know all the people in Middlesex. I don't think there are any --

MR. ALEXANDER: Wouldn't happen, sir.

SEN. LEAHY: But let's say you do. At that point, do you have to go to FISA for a warrant if you're going to continue monitoring that person, that individual?

MR. ALEXANDER: Actually, the --

SEN. LEAHY: Somebody have to go to FISA --

MR. ALEXANDER: Somebody -- potentially, but not necessarily. And the question really gets us to where are we in the process of knowing that that is a terrorist. If we know for sure that's a terrorist, it's gone to the FBI, the FBI would take that, probably to a FISA, and start their own procedures, with the lead in investigative information that we gave them.

Generally, you don't have a clear-cut case like that, sir.

SEN. LEAHY: And I was trying to make it -- for an easier answer, to make it clear-cut.

Well, let's go to Section 9(k) of the chairman's bill. This would exempt from criminal liability any FBI agent or intelligence officer who executes a physical search for foreign intelligence information if the search is authorized under the Constitution. Apparently that's a reference to the president's claimed inherent authority as commander in chief.

Does this immunize anyone who conducts warrantless searches of American homes and offices without court orders under the say-so of the president?

MR. : Yeah, Steve, you want to answer that one?

MR. BRADBURY: Well, I think, Senator, it simply conforms the law to what the law -- that FISA's trying to do -- SEN. LEAHY: No, no, no, no, no. Let's go back. You were so good before answering the question right to begin with. If -- does this immunize somebody who conducted a warrantless search of an American home or office under the say-so of the president? I mean, that should be simple.

MR. BRADBURY: Well, if intelligence officers have executed surveillance programs that have been duly authorized by the president, this would recognize that those intelligence officers who exercise those authorities should not be subject to criminal process.

SEN. LEAHY: So -- and so it immunizes this --

MR. BRADBURY: I would say, Senator, that that is the approach that FISA takes today. The officers and agents of the U.S. who --

SEN. LEAHY: This is different. This is on 9(k) saying if they are authorized by the president -- the president, not FISA, but the president -- does that immunize them?

MR. BRADBURY: Well, the legislation would recognize that there may be instances where there are programs authorized by the president. That's recognized in the legislation, and then there are procedures in place for judicial review.

SEN. LEAHY: Okay.

MR. BRADBURY: There are also procedures for the attorney general in temporary circumstances to authorize surveillance without a court order. And so --

SEN. LEAHY: Well, has the president authorized warrantless physical searches outside of FISA?

MR. BRADBURY: I think that the only thing the president has talked about is the terrorist surveillance program. That's the program that is done today without a FISA order. And that's been the subject of the hearings before this committee. And I think it's an appropriate subject for the legislation that's been proposed.

SEN. LEAHY: Can you answer the question whether he's authorized such warrantless searches?

MR. BRADBURY: I'm not going to say he has.

SEN. LEAHY: I wanted to make sure you had a chance to respond on that specifically.

You know, I worry that what we're doing is trying to immunize a lot of activities, sort of like we had this great battle here, conducted on the pages of the press and all, on the question of torture. And then after wonderful signing ceremonies at the White House and everything else, the president said, "However, there will be areas where we don't have to apply that law," and thus agreed to immunize people.

I worry -- but it's not going into this question of immunization -- I'm not talking about the president's pardon ability, and we've seen that in Watergate and others, where the president has pardoned people afterward. But -- and Iran-contra and so on. I'm talking about blanket immunization.

Let me ask both General Alexander and General Hayden this. As I understand FISA, it's always allowed NSA to use a kind of vacuum cleaner approach to radio communications in the United States, sometimes referred to the NSA exemption. So in the chairman's bill, if you repeal Section 101(f)(2) of FISA, would that extend the NSA exemption to all electronic communications, both wire and radio?

(Off-mike conferral among witnesses.)

MR. : Again, I think the straightforward answer, Senator, is yes, and just then one additional sentence of explanation is that it would allow NSA to target foreign entities.

And we've, in our discussions, I think have crossed some concepts here. In terms of targeting a foreigner for a foreign intelligence purpose, the chairman's bill would allow NSA to use all the tools that it has; it would not make a distinction between grabbing a signal out of the air or grabbing a signal some other way.

SEN. LEAHY: Yeah, I understand. So, for example, if you had -- this would allow you to seize, record, say, all the calls between the United States and India, just blanket.

MR. ALEXANDER (?): You would -- you would -- no, it would not.

SEN. LEAHY: I mean, I'm talking about under the -- if you repeal Section 101(f)(2).

MR. ALEXANDER (?): No, no, not at all. It would allow you to target a phone number in Central Asia, all right, and it would give you the same ability to cover that target that you now have, pulling that signal out of the air or collecting that signal overseas, it would allow you to use all the tools that we have at our disposal in order to get what we've already agreed is coverage of a legitimate foreign intelligence target.

SEN. LEAHY: Do we do this kind of vacuum-cleaner surveillance of Americans now?

MR. ALEXANDER (?): You're talking about intercepting the content or -- Senator, everything is done, it is targeted and for a foreign intelligence purpose. No.

SEN. LEAHY: If on these calls -- and I understand, without going into the specifics of the program, you've taken a huge number of calls not -- and e-mails, not specifically on a person. Are those then stored for retrieval and analysis by NSA --

MR. ALEXANDER (?): Sir -- Senator, your premise is incorrect.

SEN. LEAHY: Okay.

MR. ALEXANDER (?): Under the president's program, when NSA collects the content of a communication, it has already established a probable cause predicate that one or both communicants is associated with al Qaeda. So we do not vacuum up the contents of communications, under the president's program, and then use some sort of magic after the intercept to determine which of those we want to listen to, deal with or report on.

SEN. LEAHY: What if something is picked up by mistake? What happens to it?

MR. ALEXANDER (?): There's a technical term called "inadvertent collection." If NSA collects something inadvertently, standard procedures for the president's program are the standard procedures we have for all inadvertent collection -- it is destroyed.

SEN. LEAHY: So it's not available to others throughout the government?

MR. ALEXANDER (?): Only with one exception. If the inadvertent collection contains evidence of a crime, policy and statute require us to report that. Otherwise, it's destroyed.

SEN. LEAHY: Okay. Now, in addition to narrowing the definition of electronic surveillance, as I read Section 9, it would expand the so-called embassy exception, in Section 102 of FISA. Am I correct on that, Mr. Bradbury?

MR. BRADBURY: Yes, Senator. I believe under this new provision, that provision would allow the attorney general to approve for a period targeted foreign intelligence surveillance that is directed solely at the communications of foreign government operations or non- U.S. persons who are agents of a foreign government -- solely at those communications.

SEN. LEAHY: But if this was passed -- for example, you have a congressional staffer call the German embassy to plan a congressional trip to Berlin, that could be picked up?

MR. ALEXANDER (?): Senator, across the board, when NSA conducts surveillance against a legitimate foreign intelligence target and that target is in communication with an American, the American is not the target, the foreign entity is the target. We have well-established procedures to protect the privacy of the U.S. communicant.

SEN. LEAHY: Well, we have Section 9 of the chairman's bill expands the definition of agent of foreign power.

We expanded that definition a few years ago, the so-called lone-wolf amendment. It also changes the definition of attorney general from being restricted to "the attorney or deputy attorney general" to "any person or persons designated by the attorney general." Would that permit the attorney general to delegate to every FBI agent and intelligence officer in the country the authority to authorize emergency wiretaps of phone calls?

MR. BRADBURY: No, Senator. That's not the way the attorney general delegates his authority. So, for example --

SEN. LEAHY: But would he -- under this change of definition to now include any person or persons designated by the attorney general, I'm not saying whether he would do it, but would he have that power?

MR. BRADBURY: He would never do that. He would never do --

SEN. LEAHY: Would he have the power?!

MR. BRADBURY: Not under his current regulations.

SEN. LEAHY: This is like you buy a car that can go 125 miles an hour; you're going to say, "But of course, I'll never drive it over the speed limit," but you could go 125 miles an hour. If this says he can delegate it to anybody, does he have the power to delegate it to anyone?

MR. BRADBURY: He would delegate pursuant to his existing regulations on delegations, which are limited. And so in this case, for example, you'd be talking about the assistant attorney general for the National Security Division, in all likelihood.

SEN. LEAHY: But we have in the law now it's restricted to the attorney general or the deputy attorney general, as -- (inaudible) -- reference to that in Ruth Marcus's column this morning in the paper. But this would allow -- permit him to go way beyond that, does it not? I mean, just on the face of it, aside from what he might or might not do, on the face of it does it allow him to go way beyond that?

MR. BRADBURY: Well, Senator, let me say this. All authorities of the attorney general today under statute, unless they're expressly limited against delegation, are subject to delegation by the attorney general pursuant to his existing regulations in the Department of Justice, and this would simply allow for that. But under those regulations, authorities of the attorney general are not widely delegated to all individual FBI agents, for example. That is simply not done, and it wouldn't be done.

SEN. LEAHY: I had such hopes for you earlier when you actually answered a question yes or no.

But I'll submit the rest of my questions, Mr. Chairman. You know, this is highly technical. Between the House and Senate, I remember we had more than a dozen hearings when we considered reauthorization of the Patriot Act, and this bill goes way beyond the Patriot Act. So we will require more answers. And I appreciate the extra time.

SEN. SPECTER: Well, Senator Leahy, we're available for more hearings. We've only had five. We'll have as many as we need.

General Hayden, thank you for your testimony and thank you for your service. General Alexander, thank you for your testimony and for your service. Mr. Bradbury, thank you for your testimony and your service. It's good to have real professionals come before this committee and answer the questions.

MR. BRADBURY: Thank you, Mr. Chairman, and thank you, Senator Leahy.

END.

Exhibit 16

# House Permanent Select Committee on Intelligence

# Hearing on the Protect America Act 0f 2007

**September 20, 2007**

**Statement for the Record**

**of**

**J. Michael McConnell**

**Director of National Intelligence**

STATEMENT FOR THE RECORD OF
J.MICHAEL McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES

September 20, 2007

Good morning Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee:

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector. I am pleased to be joined here today by Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and am sensitive to the fact, that FISA and the Protect America Act and the types of activities these laws govern, are of significant interest to Congress and to the public. For that reason, I will be as open as I can, but such discussion comes with degrees of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities. Therefore, on certain specific issues, I am happy to discuss matters further with Members in a classified setting.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

## The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented

Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

**Technology Changed**

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain “in wire” or fiber optic cable transmissions fell under FISA’s definition of electronic surveillance. Congress’ intent on this issue is clearly stated in the legislative history:

> “the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.”

Thus, technological changes have brought within FISA’s scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA’s requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

**National Security Threats**

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

## What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and

- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

**Common Misperceptions About the Protect America Act**

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only “foreign-to-foreign” communications from FISA’s scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is who the target is, and where the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

## Oversight of the Protect America Act

### Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General

Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to this Committee and the Senate Intelligence Committee regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of the Senate and House Judiciary Committees, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of this Committee requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed staff members of this Committee regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four staff members of this Committee for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from this Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from the Senate Intelligence Committee and two staff members from the Senate Judiciary Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ’s National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from this Committee, and the Senate Intelligence, Judiciary and Armed Services Committees regarding the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on this Committee and four of that Committee’s staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four staff members of this Committee and this Committee’s Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House

Judiciary Committee staff member. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

Additional Member and staff briefings are scheduled to take place this week.

**Lasting FISA Modernization**

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

Making the Changes Made by the Protect America Act Permanent

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed, however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will ensure that the Executive Branch has sufficient time in an emergency situation to prepare an application, obtain the required approvals of senior officials, apply for a Court order, and satisfy the court that the application should be granted. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

# Exhibit 17

Department of Justice

STATEMENT OF

KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 20, 2007

**STATEMENT OF**
**KENNETH L. WAINSTEIN**
**ASSISTANT ATTORNEY GENERAL**
**NATIONAL SECURITY DIVISION**
**DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

**SEPTEMBER 20, 2007**

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as “FISA”).

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration’s proposal. While I commend Congress for passing the Protect America Act of 2007 (the “Protect America Act”) in August, the Act is a partial solution that will expire in less than six months. We urge the Congress to make the Protect America Act permanent, and also to enact the other important reforms to FISA contained in the Administration’s proposal. It is especially imperative that

Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several concerns and misunderstandings that have arisen regarding the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

## The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[1] The law authorized the Attorney General to make an application to a newly established court—the Foreign Intelligence Surveillance Court (or "FISA Court")—seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the

[1] H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."[2]

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which Government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that its drafters never intended.)

The original definition of electronic surveillance is the following:

> (f) "Electronic surveillance" means-
>
> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from

[2] *Id*. at 27.

> a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[3]

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition of "the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA's scope, period.

Further analysis of that definitional language also demonstrates the opposite—that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as "radio" (vs. "wire") communications. Under the statutory definition, surveillance of these international/"radio" communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of "electronic surveillance");[4] or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that "both the sender and all intended recipients are in the United States").[5] Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in "electronic surveillance" and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

---

[3] 50 U.S.C. 1801 (f).
[4] 50 U.S.C. 1801 (f)(1).

As satellite ("radio") gave way to transoceanic fiber optic cables ("wire") for the transmission of most international communications and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA's scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government's efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA's reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

---

[5] At the time of FISA's enactment, the remaining two definitions of "electronic surveillance" did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to "wire communications," which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA's drafters explained was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." H.R. Rep. No. 95-1283 at 52.

The legislative package we submitted in April proposed to fix this problem by amending the definition of "electronic surveillance" to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA's privacy protections on persons located in the United States.

## The Protect America Act of 2007

Although Congress has yet to conclude its consideration of the Administration's proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration's proposal. It is particularly critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the information from or with the assistance of a communications service provider, custodian, or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B concern persons reasonably believed to be outside the United States and therefore do not constitute electronic surveillance. The FISA Court then must review the Government's determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us to close existing gaps in our foreign intelligence collection that were caused by FISA's outdated provisions.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide reporting to Congress about our implementation and use of this new authority that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

We already have completed two compliance reviews and are prepared to brief you on those reviews whenever it is convenient for you.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Concerns and Misunderstandings about the New Authority

I also want briefly to address some of the concerns and misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of this Committee during the September 6, 2007, hearing, we sent a letter to the Committee that clearly outlines the position of the Executive Branch on several such issues. We hope that the letter dispels any concerns or misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement.

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. As I explained at a hearing of the House Judiciary Committee on September 18, 2007, the Act leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." I reiterated this conclusion at the House Judiciary Committee hearing on September 18, 2007—the statute simply does not authorize these activities.

Section 105B was intended to provide a mechanism for the government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, this provision does not authorize the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, some have expressed concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA—because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1)—and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect

America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. I reiterated this position at the House Judiciary Committee hearing on September 18, 2007. Because it would remain a violation of FISA, the Government cannot—and will not—use this authority to engage in "reverse targeting."

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in "reverse targeting." If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target's calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target's communications.

Additionally, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA's scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community's long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order

12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in

1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas—a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

## The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. Second, Congress should provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. Third, it is important that Congress consider and ultimately pass other provisions in our proposal. These provisions—which draw from a number of thoughtful bills introduced in Congress during its last session—would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of "agent of a foreign power"—a category of individuals the Government may target with a FISA court order—to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.

- The bill would provide a mechanism by which third parties—primarily telecommunications providers—could challenge a surveillance directive in the FISA Court.

- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. Additionally, it is critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. This important provision is contained in section 408 of our proposal. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill—both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent.

Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States As detailed above, when FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, “electronic surveillance” would encompass: “(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.”

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community's ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of “foreign powers” to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of “minimization procedures” referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. This is a critical change that works hand in glove with the new definition of “electronic surveillance” in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of “electronic surveillance,” certain activities that previously were “electronic surveillance” under FISA would fall out of the statute’s scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction. The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

Section 404

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this Committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it “contains significant foreign intelligence information.” This ensures that the Government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 406 also would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

## Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term “weapon of mass destruction.” Subsection 407(a) also amends the section 101 definitions of “foreign power” and “agent of a foreign power” to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.” Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

## Section 408

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches.

Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Other Provisions

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration.  It would allow for a smooth transition after the proposed changes take effect.

Section 414 provides that any provision in sections 401 through 414 held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections.

## Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner.  The Protect America Act is a good start, but it is only a start.  In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April.  It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.  These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans.  We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal.  I look forward to answering your questions.

HEARING OF THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE SUBJECT: THE FOREIGN INTELLIGENCE SURVEILLANCE ACT CHAIRED BY: REPRESENTATIVE SILVESTRE REYES (D-TX) WITNESSES: DIRECTOR OF NATIONAL INTELLIGENCE MIKE MCCONNELL; KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL IN THE DEPARTMENT OF JUSTICE'S NATIONAL SECURITY DIVISION LOCATION: 1300 LONGWORTH HOUSE OFFICE BUILDING, WASHINGTON, D.C. TIME: 9:14 A.M. EDT DATE: THURSDAY, SEPTEMBER 20, 2007

---

REP. REYES: (Sounds gavel.) The committee will please come to order. Today the committee will receive testimony from the director of national intelligence, Admiral Michael McConnell, and the assistant attorney general for national security, Mr. Kenneth Wainstein, who is -- who we're waiting on now -- concerning the Foreign Intelligence Surveillance Act, and the recently enacted legislation that expanded the administration's surveillance powers; the Protect America Act, or as commonly referred to, the PAA. We are here today to discuss this legislation and deal with one of the -- what I think is one of the most critical issues of our time. We need to balance measures intended to protect the homeland with preserving civil liberties.

So in that respect I want to welcome our witness, Admiral McConnell, and when Mr. Wainstein gets here as well, to our hearing here.

I believe that getting this right is fundamental to the proper functioning of this great democracy, and I believe that Congress must do everything that it can to give the intelligence community what it needs to protect America, at the same time ensuring that we do not abandon the fundamental principles of liberty that underpinned our Constitution.

For more than 200 years we have managed to have both liberty and security. And I intend to do my part to ensure that we continue to maintain this careful balance in the years to come.

This brings me to the recent modifications to FISA that Congress passed on the eve of our August recess legislation that I believe alters that precious balance between liberty and security in an unnecessary and perhaps even dangerous way.

I want to begin by setting the record straight about the concerns that have been raised over the expansive scope of the new law. There has been a lot of rhetoric from the administration and some in Congress suggesting that critics of the new act are placing the rights of foreigners and terrorists before the need to protect America.

Our position shouldn't be characterized as seeking to protect the rights of foreigners, plain and simple. Our concerns are about protecting the rights of Americans, not foreigners abroad. Thus we are concerned for the privacy of Americans who may happen to be communicating with someone abroad.

To be clear when a doctor living in Los Angeles calls a relative living abroad I am concerned about her rights. When a soldier serving in Iraq or Afghanistan emails home to let his family know that he made it back from his latest mission, I am concerned about his rights and the rights of his family.

But under the new law we have allowed the government to intercept these calls and these emails without a warrant, and without any real supervision from the judicial branch. In doing so we have unnecessarily put liberty in jeopardy by handing unchecked power to the executive branch.

I say unnecessarily because there was no need to do this in this particular way. There was an alternative, but the administration chose to torpedo it. With that, let me explain. In late July the director of the national intelligence came to us and identified a specific gap which he described publicly as a backlog with respect to the FISA process that he claimed had placed our country in a heightened state of danger.

At first he said that he needed two things: number one, a way to conduct surveillance of foreign targets in a block without individual determinations of probable cause; and two, a way to compel communications carriers to cooperate. We gave him both those powers.

After we shared our draft legislation with him, he came back to Congress and said that he wanted three more things. We again agreed, and tailored our bill to provide each of these three things. That bill, H.R. 3356, was a result of substantial and I believed at the time good faith negotiations with Admiral McConnell.

We gave Director McConnell everything he said that he needed to protect America. But it also did something else; it also protected our Constitution.

Yet at the final hour, and without explanation, after having repeatedly assured us that the negotiations had been in good faith, the administration rejected that proposal. Director McConnell not only rejected it, he issued a statement urging Congress to vote it down, claiming that it would not allow him to carry out his responsibility to protect our nation.

Director McConnell, today in your testimony I would like to hear your side of this story. I want to hear why it is that even though we tailored legislation to meet your requirements you still rejected it.

I want to hear why you believe that H.R. 3356 would not have allowed you to do your job and why you issued a statement to that effect on the eve of the House vote.

I want to know what specifically you believe was lacking in H.R. 3356.

And most importantly, Admiral McConnell, I want to know what it is about the inclusion of proper checks and balance and oversight in our bill that you found so unacceptable.

These are important questions because Congress intends to enact new legislation as soon as possible as are replacement to the administration's bill. In early October at the speaker's request this committee will mark up FISA legislation to address the needs of our intelligence community. The new legislation will deal with the deep flaws in the administration's bill, the vague and confusing language that allows for warrantless physical searches of Americans' homes, offices and computers; then conversion of the FISA court into what we believe is a rubber stamp; and the insufficient protections for Americans who are having their phone calls listened to and emails read under this new authority as we speak here today. Before closing I want to take this opportunity to reiterate a critically important request for documentation regarding the NSA surveillance program that still remains outstanding. As I have said before, to date the administration refuses to share critical information about this program with Congress. More than three months ago ranking member Hoekstra and I sent a letter to the attorney general and the DNI requesting copies of the president's authorizations, and the DOJ legal opinions. We have yet to receive this information.

Congress cannot and should not be expected to legislation on such important matters in the dark. I would hope that Admiral McConnell, you and Mr. Wainstein when he gets here will help us in getting this material so that we can have a clear understanding of the issues that we're dealing with as a committee.

So I look forward to this hearing, and I want to now recognize the ranking member for any statement that he may wish to make.

REP. PETER HOEKSTRA (R-MI): Thank you, Mr. Chairman.

Good morning, good morning, Director McConnell, and appreciate your being here.

Also appreciate all the work that you did back in July, make sure that we got a bill through the House and through the Senate to the president's desk that enabled us to provide the NSA, the intelligence community, with the flexibility, the agility, and the tools that it needed to keep us safe.

You know we -- Republicans weren't invited to be a part of the negotiations as the Democratic bill was developed. And you know that was a disappointing effort. Most of the time things on the intelligence committee, we tried to do these things in bipartisan ways. But since we weren't part of the process the only thing we could do is take a look at the end results. And there is no doubt that the bill that passed the House in a bipartisan basis, the bill that passed the Senate in a bipartisan basis, did exactly what you had identified needed to happen, one, a bill and a piece of legislation that could become law that would give the intelligence community the tools that it needed to be successful, to keep America safe, and provided very appropriately the kind of balance that we need to protect American civil liberties.

Today's hearing highlights the critical need for speed and agility in intelligence collection. I mean one of the things that we have learned is that an intelligence community that for so many years was designed to be one step faster in the former Soviet Union and the threat that came from the former Soviet Union, was not going to be good enough to face the threat that we face from radical jihadists today. And so the changes that we need, and the changes that were made, were designed to keep and to put the intelligence community in step with where technology was today and where the threat level was.

Since the president signed the bill the intelligence community has succeeded in closing that intelligence gap you identified in July -- excuse me. There should be no significant disagreement that the Protect America Act has improved our intelligence capabilities, made our country safer.

And regardless of the specific authorities used, the recent terrorism-related arrests in Germany and Denmark demonstrated why timely intelligence collection is so critical, and why we must ensure that the professionals are our intelligence agencies continue to have this streamlined and effective tools at their disposal.

Not only did the intelligence community effectively take and participate in taking down these threats, we also know that these threats continue. There have been a couple of bin Laden tapes. There's a Zawahiri tape, I guess that's maybe out there today. We'll have to wait for the intelligence community to verify and validate its authenticity.

There's rumors of another bin Laden tape. But you know some of us were in the -- in the war zone over the weekend. We were in Afghanistan, we were in Pakistan, we were in Iraq. And we talked to the intelligence folks and our folks on the ground. And we asked them about the threat, and said, hey, is there any way that, you know, we possibly miscalculated this threat, that it's overblown. And consistently the people have come back and said, no, this threat is real.

And one of the comments that came out that kind of sticks with me is, one of our folks said, you know, we see threats all the time, we're working on threats all the time. And these are the kinds of things I wouldn't want my parents to know about, the kinds of things that these people would like to do against the homeland.

And that's why it's important that America not afford to go dark and reopen the intelligence gaps -- (inaudible) -- under FISA.

You know earlier this week the committee received testimony, information from the administration, other outside groups, that I hope have put to rest the myth that the Protect America Act somehow reduces civil liberties protections for Americans.

As Director McConnell and Mr. Wainstein will again I think reaffirm today, the law does not permit reverse targeting of Americans, or the searches of the homes and businesses of ordinary citizens that some have breathlessly claimed is contained in the bill. The Department of Justice has made it clear that it believes it must seek a court order to target the communications of Americans, and the committee will continue to carefully ensure that it does so.

The -- you know we also learned that some of the activist special interest groups that testified see not to preserve the structure of FISA as we have known it, but instead, want to impose substantial and crippling new restrictions on our intelligence agency. If you go back and you read some of the testimony, it is clear. They do want to provide the civil liberties protections that we give to American citizens and people residing within our borders, they want to extend those rights to foreign individuals including foreign terrorists, and that is the sum and total of what they intend to do.

With that, Mr. Chairman, I will submit my entire statement for the record and yield back the balance of my time.

REP. REYES: Without objection. And we have been joined by Mr. Wainstein. Mr. Wainstein, welcome to the hearing. We appreciate your participating here this morning.

MR. WAINSTEIN: Thank you, Mr. Chairman.

REP. REYES: With that, Director McConnell -- did you have a question, Mr. Issa.

REP. DARRELL ISSA (R-CA): I'd like to just make a brief opening statement. One minute.

REP. REYES: Okay, Mr. Issa is recognized for one minute.

REP. ISSA: Thank you, Mr. Chairman. And I will submit my formal opening statement for the record. But I do think that something needs to be cleared up in real time. During your opening statement, Mr. Chairman, I think unintentionally you talked about soldiers phoning or emailing home. And I think it's important to have in the record that in fact in World War II, in fact in Korea, and in fact in Vietnam, no soldier had an expectation that his phone calls or his emails -- which didn't exist then, but his regular mails -- were not going to be potentially censored.

And in fact some -- one only has to watch an old version of Mash to see what things looked like after they went through scrutiny on mail to find out whether or not it might divulge information from the battlefield.

So I would hope that when we go through this dialog we not use our soldiers, risking their lives and limb, as somehow a group that expects not to have communication heard. Just the opposite I would say that our men and women uniform are the first to say, I'm not worried about what you listen to or email coming from the battlefield. Just the opposite. I need to be kept safe by making sure that in fact we do secure that kind of information coming from Afghanistan and Iraq.

So I know the chairman is a soldier himself and didn't intend to misstate that. But I thought it had to be put into the record, and I yield back.

REP. REYES: I want to thank my colleague from California for clarifying the fact that we may be spying on our soldiers.

With that, Director McConnell, you are recognized for your opening statement.

MR. McCONNELL: Thank you, Senator, ranking member Hoekstra, members of the committee, a pleasure to appear before you today.

I appreciate the opportunity to discuss the Protect America Act-- I will refer to it as PAA -- and the need for lasting modernization of the Foreign Intelligence Surveillance Act of course we'll refer to as the FISA.

I'm pleased to be joined today by Assistant Attorney General Ken Wainstein of the Department of Justice national security division.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. AS the head of the nation's intelligence community, it is not only my desire but in fact my duty to encourage changes to policies and procedures, and where needed, legislation to improve our ability to provide warning of terrorist or other attacks to the country. On taking up this post it became clear to me that our foreign intelligence capabilities were being degraded. I learned that collection using authorities provided by FISA continued to be instrumental in protecting the nation, but due to changes in technology, the law was actually preventing us from collecting foreign intelligence.

I learned that members of Congress in both chambers, and on both sides of the aisle had in fact proposed legislation to modernize FISA, and this was accomplished in 2006. In fact a bill was passed in the House in 2006.

And so the dialog on FISA has been ongoing for some time. This has been a constructive dialog, and I hope it continues in the furtherance of serving the nation to protect our citizens.

None of us want a repeat of the 9/11 attacks, although al Qaeda has stated their intention to conduct another such attack.

As is well known to this committee, FISA is the nation's statute for conducting electronic surveillance -- a very important term, electronic surveillance. That is some of our disagreement on interpretation, and we'll have more to say about that later.

Then other part of the act is for physical search, for foreign intelligence purposes. When passed in 1978, FISA was carefully crafted to balance the nation's need for collection of foreign intelligence information with the need to provide protection for civil liberties and privacy rights of our citizens.

There were abuses of civil liberties from the 1940s to the 1970s that were galvanized by the abuses of Watergate that led to this action we call FISA. The 1978 law created a special court, a foreign intelligence surveillance court, to provide judicial review of the process. The court's members devote a considerable of their time and effort while at the same fulfilling their district court responsibilities. We are indeed grateful for their service.

FISA is very complex. Therein the problem: it is extremely complex. And in our dialog today what we'll examine is if you insert a word or a phrase it has potentially unintended consequences. And that is the sum of our disagreement over not being able to examine unintended consequences due to the press of time.

It is a number of substantial requirements, detail applications contain extensive factual information that require approval by several high ranking officials in the executive branch before it even goes to the court.

The applications are carefully prepared, and they're subject to multiple levels of review for legal and factual sufficiency. It is my steadfast belief that the balance struck by the Congress in 1978 was not only elegant, it was the right balance to allow my community to conduct foreign intelligence while protecting Americans. Why did we need the changes that the Congress passed in August? FISA's definition -- and I mentioned this earlier -- of electronic surveillance simply did not keep pace with technology. Let me explain what I mean by this.

FISA was enacted before cell phones, before email, and before the Internet was a tool used by hundreds of millions of people to include terrorists.

When the law was passed in '78 almost all local calls in the United States were on a wire, and almost all international calls were in the air, known as wireless. Therefore FISA was written in 1978 to distinguish between collection on wire and collection out of the air.

Today the situation is completely reversed. Most international communications are on a wire, fiber optic cable, and local calls are in the air. FISA was originally -- FISA also originally placed a premium on the location of the collection. There was the cause of our problem, on a wire, in the United

States, equal a warrant requirement even if it was against a foreign person located overseas.

Because of these changes in technology communications intended to be excluded from FISA in 1978 were in fact frequently included in 2007. This had real consequences. It meant the community in a significant number of cases was required to demonstrate probable cause to a court to collect communications of a foreign intelligence target located overseas. And that's very important, and I would emphasize it. Probable cause level of justification to collect against a foreign target located overseas.

Because of this, the old FISA's requirements prevented the intelligence community from collecting important intelligence information on current threats.

In a debate over the summer, and since, I've heard individuals both inside the government and outside assert that the threats to our nation do not justify this authority. Indeed, I've been accused of exaggerating the threat that the nation faces. Allow me to attempt to dispel that notion.

The threats that we face are real, and they are serious. In July of this year we released the National Intelligence Estimate, we refer to it as the NIE, on the terrorist threat to the homeland. The NIE is the community's most authoritative written judgment on a particular subject. It is coordinated among all 16 agencies of the community.

The key judgments from this NIE are posted on a website, and I would encourage all to review the full details.

In short the NIE's assessments stated the following. The U.S. homeland will face a persistent and evolving terrorist threat over the next three years. That's the period of the estimate. The main threats come from Islamic terrorist groups and cells, and most especially al Qaeda.

Al Qaeda continues to coordinate with regional groups, such as al Qaeda in Iraq, across northern Africa and in other regions. Al Qaeda is likely to continue to focus on prominent political, economic and infrastructure targets with the goal of producing mass casualties. And I repeat for effect -- with the goal of producing mass casualties. Also the goal is visually dramatic destruction, significant economic aftershock and fear in the U.S. population. These terrorists are weapons-proficient, they're innovative and they're persistent. Al Qaeda will continue to try to acquire chemical, biological, radiological and nuclear material for attacks. And if achieved, they will use them given the opportunity to do so.

Global trends and technology will continue to enable even small numbers of alienated people to find and connect with one another, justify their anger, even intensify their anger and mobilize resources to attack, all without requiring a centralized terrorist organization, training camp or leader. This is the threat we face today and one that our community is challenged to counter.

Moreover, these threats we face are not limited to terrorism. Countering the proliferation of weapons of mass destruction is also an urgent priority, and FISA most frequently is the primary source of information in that area. The Protect America Act updating FISA, passed by Congress and signed into law by the president on the 5th of August, has already made the nation safer. After the law was passed, we took immediate action to close critical gaps related to terrorist threats. The act enabled us to do this, because it contained the five following pillars. It clarified the definition of electronic surveillance under FISA in that it should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. Second, under the act, we are now required to submit to the FISA court for approval, the procedures we use to determine that a target of the acquisition is a person outside the United States. This portion is new and was added to give the Congress and the public more confidence in the process. In addition to oversight by the Congress, the new FISA procedures involving foreign threats are now overseen by the court. The act allows the attorney general and the DNI to direct communication providers to cooperate with us to acquire foreign intelligence information. The act also provides liability protection proscriptively for private parties who assist us when we are directing with a lawful directive to collect foreign intelligence information. And most importantly -- most importantly to this committee and certainly to me -- FISA, as amended by the Protect America Act, continues to requires that we obtain a court order to conduct electronic surveillance or physical search against all persons located inside the United States.

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that continue to need attention. For reasons that I've outlined today, it's critical that the FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside the United States. Second, I call on Congress to act swiftly to provide retroactive liability protection to the private sector. It is important to keep in mind that the intelligence community often needs the assistance of the private sector to protect the nation. We simply cannot go alone. We must provide protection to the private sector so that they can assist the community in protecting the nation while adhering to their own corporate fiduciary duties. Thirdly, in April 2007 in the bill that we submitted to Congress, we asked for a number of streamlined provisions that would make processing FISA applications more effective and efficient. These changes would substantially improve the FISA process without affecting the important substantive requirements of the law. Finally, we understand and fully support the requirement for the community to obtain a court order or a warrant any time the target for foreign surveillance is located inside the United States. That was true in 1978 when the law was originally passed. It is true today with the update that became law last month.

Mr. Chairman, that completes my remarks. I'd be happy to answer your questions.

REP. REYES: Thank you, Admiral.

With that, we recognize Mr. Wainstein for his opening statement.

MR. WAINSTEIN: Chairman Reyes, Ranking Member Hoekstra and members of the committee, good morning and thank you very much for this opportunity to testify before you again concerning FISA modernization. I'm proud to be here to represent the Department of Justice, and I'm happy to discuss this important issue with you.

The Protect America Act is an important law that has allowed the intelligence community to close intelligence gaps caused by FISA's outdated provisions, and it has already made a difference, it has already made our nation safer. In my statement this afternoon, I'll briefly explain why I believe Congress should make the Protect America Act permanent and also enact other important reforms to the FISA statute. But before I do that, I would like to thank this committee for having me in closed session last week.

And in particular, I'd like to thank you, Chairman Reyes, for proposing that we send you a letter laying out our position on some of the concerns that you and other members of the committee had with certain parts of the Protect America Act, concerns that certain language might permit the government to conduct intelligence activities well beyond those that Congress contemplated when it passed the statute. As the committee is aware, we drafted and sent you that letter last Friday, and it laid out why it is that we don't think those concerns will become a reality in practice. I appreciated the opportunity to engage in that dialogue with you and your colleagues, Chairman Reyes, and I look forward to continuing it here today. I believe that this process will help to reassure Congress and the American people that the act you passed in August is a measured and sound approach to a critically important issue facing our nation.

Let me turn briefly now to why I believe the act should be made permanent. As I explained in my prior testimony, in 1978, Congress designed a judicial review process that applied primarily to surveillance activities within the United States where privacy interests are the most pronounced and not to overseas surveillance against foreign targets where (cognoscible ?) privacy interests are minimal or nonexistent. They did this very much intentionally as they were working against a constitutional backdrop articulated in case law and in legislation that did not extend 4th Amendment protections to foreigners overseas and that left the conduct of foreign intelligence surveillance against foreigners overseas within the ambit and authority of the executive branch.

With this historical backdrop in mind, Congress created a dichotomy in the statute, a dichotomy between domestic surveillance that is governed by FISA, and is therefore subject to FISA court review and approval, and overseas surveillance against foreign targets that is not. Congress established this dichotomy by distinguishing between wire communications which included most of the local and domestic traffic in 1978 and which were largely brought within the scope of the statute and radio communications which included most of the transoceanic traffic of the time and were largely left outside the scope of the statute.

As a result of the revolutions in telecommunications technology over the last 29 years, much of the international communications traffic is now conducted over fiber optic cables which qualify as wire communications under the statute. As a result, many of the surveillances directed at persons overseas which were not intended to fall within FISA became subject to FISA requiring us to seek court authorization before initiating surveillance and effectively conferring quasi-constitutional protections on terrorist suspects overseas. This process impaired our surveillance efforts and diverted resources that were better spent protecting the privacy interests of Americans here in America.

As the committee is aware, the administration had submitted to Congress a comprehensive proposal in April that would remedy this problem and provide a number of other refinements and important changes to the FISA statute. While Congress has yet to act on that complete package, your passage of the Protect America Act was a very important step in the right direction. It amended FISA to exclude from its scope those surveillances directed at persons outside the U.S. And this has allowed the intelligence community to close critical intelligence gaps that were caused by the outdated provisions of FISA, and it has already made our nation safer.

But the legislation is expected to expire in just a little over four months. And we urge Congress to make the act permanent and to enact the other important reforms contained in our comprehensive proposal. It's especially imperative that Congress provide liability protection to companies that allegedly assisted the nation with surveillance activities in the wake of the September 11th attacks.

I also want to assure the committee that we recognize that we must use the authority provided by Congress not only effectively but also responsibly. And I think our actions since Congress passed the Protect America Act demonstrate our full commitment to doing just that. As we explained in the letter we sent to the committee on September 5th, we've already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as onsite reviews by a team of folks from the ODNI as well as the National Security Division of the Department of Justice. This team has already completed its first two compliance reviews, and it will complete further audits at least once every 30 days during the renewal period of the statute to ensure complete and full compliance with the implementation procedures.

In that same letter we sent to you, we also committed to providing Congress with comprehensive reports about our implementation of this authority, reporting that goes well beyond that that is required by the statute.

We've offered to brief you and your staffs fully on the results of our compliance reviews. We will provide you copies of the written reports of those reviews, and we'll give you update briefings every month on compliance matters and on implementation of this statute in general. We're confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority and that it will demonstrate to you that you made absolutely the right decision when you passed the Protect America Act last month.

The committee is wise to hold this hearing and to explore the various legislative options and their implications for national security and civil liberties. I'm confident that when those options and implications are subject to objective scrutiny and honest debate, Congress and the American people will see both the wisdom and the critical importance of modernizing the FISA statute on a permanent basis.

Thank you, again, for allowing me to appear before you today, and I look forward to answering your questions.

REP. REYES: And thank you for your testimony, Mr. Wainstein.

The only thing that you missed -- and we apologize, because I understand that you had a hard time getting in the building, so we apologize for that -- but the only thing that you missed that probably is the most germane, most important is that we seek yours and the DNI's help in getting us the documents that the ranking member and I have requested for a number of months and are critical for our committee to understand that thinking and the process that's gone in to the terrorist surveillance program. If the two of you could help, we would appreciate that very much.

I don't think anyone disputes that the threats are real. I think everybody knows and understand the threats to our country are real. The issue is whether we carefully balance our ability to remain safe as a nation while at the same time protecting our individual rights as citizens under the Constitution.

The first question I have for you, Director McConnell, is you have told us the things that you need to improve your capabilities under FISA. Initially -- and we're going back to the three things you identified previously -- no individual warrants were targets abroad, a way to compel telecommunications companies to cooperate and individual court orders when targeting an American. I believe that H.R. 3356 gave you all those elements. When we discussed these issues with you last month, you told us then that the bill was acceptable and then only to find out later that it was rejected. So I guess the first question I have is, do you still think that H.R. 3356 doesn't offer you the things that you need by way of these three requirements? And if it doesn't, which ones does it not offer or which ones do we fall short on in 3356?

MR. McCONNELL: Thank you, Mr. Chairman. I appreciate the question and opportunity to explain.

Context if I could -- in the course of this dialogue which intensified pretty briskly toward the end of July, we exchanged between us seven different drafts. While I, one, not a lawyer, two, imposed on the lawyer team that I have -- more than 20 -- that we wanted and needed these three main points that we're trying to achieve -- no warrant for overseas, as you mentioned, getting help from the private sector and requiring -- and this is one of my major points is I thought '78 law was right -- requiring us to get a warrant if it involved a U.S. person. That was sort of my philosophical underpinning. What happens, unfortunately, the law is very, very long and extremely complex. So if someone has an issue with a part of it and they want to change a phrase or attack a part of it in the language as entered, we don't know the impact of that until we can sit down, examine it and understand it and so on. Remember, I have a team of 20 lawyers that are expert in every aspect.

Let me give you a couple of examples. There are claims and worries about reverse targeting. What does that mean? The assertion is the government wants to know about a U.S. person, someone in the country. Therefore, we would target someone overseas that might contact that person, because we wouldn't have to have a warrant to target the person overseas. So language was included to address reverse targeting. Now, what that does is introduce ambiguity and uncertainty. We don't know -- you don't know, we don't know -- how the court would interpret such language once it gets there and you build (in ?) a level of uncertainty. Also, reverse targeting is unlawful. So my view, it wouldn't be required to be inserted in the law, and I was very worried about the uncertainty. So it was just not required. That's one example. And there are a number of examples.

Let me move to minimization, words in the draft to address minimization. And what do I mean by minimization? When we are conducting surveillance against a foreign target and a foreign target called (into ?) the United States, we have to make some decision with regard to that transaction. It's been true for 30 years, it's true in the criminal side, it's an artifact of doing this business. Minimization has been examined by the court. It's found to be reasonable by the court. So in the case that a foreign terrorist was calling (into ?) the United States, if it were incidental and innocent, it would be purged from our database. If it were real, that might be the most important call that we intercepted. And so one would ask, well, now, what would you do with that? In that case, once the sleeper or someone in the country became a target of interest for probable cause, we would get a warrant. So in my view, minimization for 30 years, or almost 30 years, has worked well. And if you attempt to adjust it, you don't fully understand or appreciate the outcome.

And there were a few other things I'll just give you, not to take too much time. There was information about the definition of electronic surveillance. There are four different definitions, and what we had proposed is changing the definitions so we excluded a foreigner in a foreign country. The draft you had still included a definition of electronic surveillance to include foreign persons. So you're back in the situation of not knowing how the court would interpret it. So my problem was, one, limited time to review, get the draft, short turnaround, sit down with the lawyers, and we're coordinating between all the experts. And we'd say well, we don't know what this means. So I was put in a position where I could do nothing but say can't support it, because we haven't had a chance to examine it. That's sum and substance of what happened.

REP. REYES: Thank you, Director McConnell. I'm a bit confused or perhaps perplexed, because you're talking about a lot of things that were not included in 3356. The negotiations that we engage with you in covered those three points that you said you needed.

MR. McCONNELL: Yes, sir, they did.

REP. REYES: And expanded it even on the second go-round to include all intelligence, if you remember that issue which you made a case for making sure all foreign intelligence should be part of that process. But getting back to my original question, did 3356 give you the three things that you said you needed, that we were negotiating?

MR. McCONNELL: No, sir. The thing that I was worried about most was no warrant against a foreign target in a foreign country, because the wording in 3356, the definition left it uncertain. So you still would have the court involved. And so our problem was how would the court interpret it so it would put us back in the untenable situation.

Let me go back to the end of July, first couple of days of August.

REP. REYES: But Director McConnell, then why would you tell us at the time that we were having this discussion that it did everything that you wanted?

MR. McCONNELL: I said if it addressed the three fundamental -- remember, I'm not the lawyer. I'm the --

REP. REYES: I understand.

MR. McCONNELL: -- operator saying gotta have these three things. When you examined the words, I wasn't assured that I had the three things. And the reason I want to go back to the end of July and the first part of August -- Congress had a timetable that was driving the schedule. We exchanged seven drafts. Each turn -- and remember, I'm doing this on the Senate side also -- each turn, we were given very limited time to actually examine the draft. And when I say 20 lawyers, don't just imagine 20 lawyers sitting around a table. These are experts in aspects of this, because it's so complex. So we would have to have time to say, if you've changed a phrase -- just the modification to electronic surveillance -- what does that mean in the ultimate interpretation?

And that was the problem that we faced.

I could not with certainty believe that the very first thing I asked for -- the fundamental premise going in, which was the reason FISA was created -- no Fourth Amendment protection for foreigners that are suspected of activity that's inimical to the interests of the United States -- there's no intent to do that, but 3356 could still get you there.

Now, it's an interpretation, but because we didn't have time to sit back and have -- sit down and have dialogue on the give and take, that's why we were -- I said I can't support it. I just -- I don't have confidence it would come out the way you intended it.

REP. REYES: Well, I'll leave that for a couple of other members to pursue further.

I want to move on in the interest of time and ask you -- switch topics and ask you: In your testimony before the House Judiciary Committee on Tuesday, you made the statement that "No Americans had been targeted with electronic surveillance without a warrant." But if you recall, in your interview in the El Paso Times last month, you said that the number was 100 or fewer. I believe that there's been a lot of confusion on this one issue, so I would like to try to clarify that. Can you tell us, Mr. Director, since September the 11th, 2001, how many Americans have been targeted with electronic surveillance without a warrant?

MR. McCONNELL: I can't tell you the answer to that, because I don't know. I was asked the question earlier in the week in the committee and then I clarified my answer when I thought, maybe I'd left a misimpression. I can only talk about the period of time since I've served. The other part -- it's hearsay or there's a story and I could probably go find it out, but I just don't know.

What I was attempting to do, and what I've learned by this process, is no good deed goes unpunished. What I was attempting to do at a summary level was to provide some factual information that people could deal with to understand the magnitude of this issue. There were many, many claims about the intelligence community conducting massive surveillance against the American public -- a driftnet over the entire country looking at every issue and transaction and doing data mining. What I was attempting to give perspective to is there are thousands of foreign intelligence targets, and in the course of these thousand operations that we're conducting against foreign intelligence targets, on occasion a foreign terrorist called into the United States.

Now, when a foreign terrorist called into the United States and now there's reason to believe that there's something to do with terrorism, then we would be required to get a warrant. So in this specific instance -- starting in the January-February time frame -- given the numbers we were dealing with where it would result in some surveillance of a U.S. person, for which we got a warrant, that number was about 100 or less. That was the point of what I was attempting to do -- at a summary level provide the Congress, because you were being discussed in the press a lot of criticism about what we did pass or what you all passed and the president signed. So all my attempt was to do was to provide some context so people had a better way to understand this and appreciate it.

So don't know about 2001 -- wasn't here. I could go try to find out. If it's on my watch, none without a warrant and about 100 where we got a warrant and we had reason to believe we needed one.

REP. REYES: And I think that's part of what's led to the confusion on this issue when you said zero to the Judiciary Committee and --

MR. McCONNELL: The question was "without a warrant." Zero without a warrant. So once -- remember, a terrorist calls in. Now we have reason. We get the warrant. So zero without a warrant, 100-ish with a warrant. That was what I was trying to explain.

REP. REYES: Is there anybody accompanying you today that you can consult with to give us an idea of the number of Americans since September the 11th that have been targeted with electronic surveillance?

MR. McCONNELL: I don't know. Let me ask them and find out. (Off mike consultation.)

I can't give you a number, sir. We can probably get you a number. We'd have to provide it at a classified level. Let me just make a point, since -- you recall, I used to serve as director of NSA years ago and I've got some appreciation for process. When you're collecting information, the task for, in the collection context, is processing out the information. You could have data in a database that you don't know what's in the database. It just hasn't been examined. Remember, we're talking billions of things going on.

So the way the process is designed is at a point in time the database just -- it shorts to ground, goes off. You don't hold it anymore. The situation would be, given now that you have data and you have some reason to examine the data, if there was incidental collection against a U.S. person in the data -- it has nothing to do with any foreign intelligence reason -- now you know it, you have to destroy it. Get it out of your database. If it had foreign intelligence value -- terrorism, whatever -- now you must report it. Now, let's say it was a U.S. person inside the United States. Now that would stimulate the system to get a warrant and that's how the process would work.

Now, if you have foreign intelligence data, you publish it because it has foreign intelligence value and somebody wants the identity, there's a very structured process that you would have to go through to get approval to be aware of who that person's -- what that person's identity might be. So it is something that the work force of thousands of people are trained in. That's something they review on a yearly basis. It's something that's very structured to prevent any potential abuse of claims of spying on Americans.

REP. REYES: But is it your position that you can go back and give us the information -- again, since 9/11?

MR. McCONNELL: We can ask, sir. And what I'm highlighting for you is it'll be probably a range. One, I'm pretty sure that --

REP. REYES: Well, just the best you can do under those circumstances.

MR. McCONNELL: It'd probably be a classified answer.

REP. REYES: And we appreciate that.

The last thing -- and then I'll turn it over to our ranking member for his questions -- is when will you furnish us the documents that we've requested?

MR. McCONNELL: Sir, in my understanding there's a negotiation going on between the Judiciary Committees and the White House with regard to that documentation. I am generally aware. I've made my recommendations known. And so that's a process that's ongoing now. I don't know specifically where it is in the decision cycle. Maybe Mr. Wainstein -- he might have some additional insights. I don't know.

REP. REYES: Mr. Wainstein?

MR. WAINSTEIN: No, sir. I'm afraid I actually don't have any sort of updating information as to where those negotiations are. I know they're ongoing between various parts of the administration and various committees up on the Hill, but I really couldn't tell you what the status is at this point.

REP. REYES: Well, any assistance both of you gentlemen can give us we would very much appreciate it.

MR. WAINSTEIN: Certainly.

REP. REYES: With that, I'll recognize the ranking member for his questions. REP. HOEKSTRA: Thank you, Mr. Chairman.

Admiral McConnell, can you explain how the FISA structure has accounted for the possibility that the communications of Americans may be intercepted when targeting foreign persons? I mean, the law's been around for 1978. This is not a new problem, correct?

MR. McCONNELL: Yes, sir. That's correct.

REP. HOEKSTRA: So what -- you know, how have the folks at NSA dealt with this since 1978? How would this have been managed under the period of time -- in the Clinton administration when you were running NSA -- what are the processes and the procedures that go through this? I'm talking about collection of Americans.

MR. McCONNELL: All right, sir. First of all, it's unlawful to collect against a U.S. person without a warrant. So that's where you start.

REP. HOEKSTRA: That extends, really, since '78. If you're targeting and collecting against an American the people at NSA have gone through the rigorous training and that's always been subject to congressional oversight --

MR. McCONNELL: Yes, sir.

REP. HOEKSTRA: That you've got to get a warrant.

MR. McCONNELL: That's correct. And sir, I would even submit that I think we could have been better in the 9/11 situation had we perhaps thought about it differently. We put so much emphasis -- the community was trained and drilled and rehearsed and had such a cultural affinity with what we just described that any time it had anything to do with the United States we just didn't do it. So if Osama bin Laden himself were being tracked to Pakistan or Turkey or Europe or wherever, the minute he comes into the United States he's now a U.S. person and it's a different situation.

So the process when you are -- first of all, a community is tasked and responsible for only doing one thing: collecting foreign intelligence information. So when you're doing your foreign intelligence collection mission, there are circumstances whereby a foreigner could call into the United States -- we refer to that as incidental. When an incidental situation like that develops, the rules are it must be minimized. Once recognized and minimized, it is incidental. It must be purged from the database. That's what we've done for almost 30 years. If it turns out that it has intelligence value for whatever purpose -- terrorism, crime, whatever -- you're required to report it. Even in the report you're required to protect the identity of the U.S. person.

So that's the way the process has worked. It's called minimization. It's something that has been examined by the court, endorsed by the court and it actually originated on the criminal side where criminal investigators would have a warrant to, for example, conduct surveillance against a specific person in the mafia. That person may have incidental phone calls and nothing to do with the crime or braking law. That was called a minimization process. That's where it came from, that's how it's been used in the community.

REP. HOEKSTRA: Those protections are still in place.

MR. McCONNELL: Yes, sir. They are.

REP. HOEKSTRA: You stated in the Judiciary Committee that you were required earlier this year -- or that you were required to get a FISA order to conduct surveillance on Iraqi insurgency who had capture Americans. Can you discuss that case any further?

MR. McCONNELL: Sir, I have to be a little careful because of sources and methods issues, but the situation was -- as you know -- because global communications move on wire, you could have a situation where information would pass on a wire through this country. And so for us to specifically target the individuals that were involved in that kidnap, we had to go through a court order process. Now, when we've talked about this before people frequently say, well, wait a minute -- why didn't you just do emergency FISA? Well, that is the point. We are extending Fourth Amendment rights to a terrorist foreigner, foreign country, who's captured U.S. soldiers and we're now going through a process to produce probable cause that we would have authority to go after these terrorists. So then people say, well, why didn't you just go -- you've got emergency authorization. Well, emergency authorization doesn't mean you don't go through the process, which is probable cause, so some analyst has got to do it. Then some official's got to sign it out and it's got to come to either me or some other official, then it goes to the attorney general, then it goes to the FISA court. So even though you could go faster, some of have asserted -- well, just automate the process and you'll go the speed of light. The human brain still has to engage and you still have to certify the accuracy.

So the reason I raised the case is it's my fundamental belief that that foreigner in a foreign country, known terrorist, had no right to protections of the Fourth Amendment and the process slowed us down. That was what I was complaining about.

REP. HOEKSTRA: And the situation was one where -- you know, we ought to be clear about it. These were Americans that were captured.

MR. McCONNELL: Yes, sir.

REP. HOEKSTRA: And the way that the process required you -- it required you to go through a court process to get a FISA order to be able to listen.

MR. McCONNELL: And the reason, sir, is two things: the mode of communications that was used and where it was intercepted. That was the only issue.

Now, let's go back to the terrorist in Baghdad. If they'd had a push-to-talk phone or if they had a cell phone talking to a tower of they'd used signal flags or if they'd talked to a cell phone to a satellite -- any of that -- there's no warrant, because it's in the air and it's in a foreign country. But because they used a mode of communications that involved wire and the wire passed into the United States, that was where the technology did not keep pace -- where the law did not keep pace with technology. It was because of how and where that put us in that situation. They were using a device or devices that caused us to stop and get a warrant, so it slowed us down.

REP. HOEKSTRA: Good. Thank you.

With that, Mr. Chairman, I'll yield back the balance of my time.

REP. REYES: I thank the ranking member.

Just to be clear on this particular case that you mentioned, the emergency provisions -- and we've had testimony to this effect -- kick in so you can start monitoring immediately.

MR. McCONNELL: Yes, sir.

REP. REYES: And then you evaluate whether or not within those 72 hours you're going to need to take it to FISA. MR. McCONNELL: Sir, I didn't make myself clear. I'm sorry I'm failing here.

Here's my point: Emergency provisions still have to meet a probable cause standard. So I can have an emergency provision. I still have to go through the process of probable cause, get people to certify and take it to a court. My argument is that it's a foreigner, foreign country, shouldn't be worried about emergency process or probable cause. It's a foreigner in a foreign country. That's our mission. We should be doing that without involving the court. That's the point I'm trying to highlight.

REP. REYES: Okay. I understood your point, but I just wanted to make sure we were clear so that the American people don't misunderstand that everything wasn't done as quickly as possible.

MR. McCONNELL: Could we have gone faster? No question! I'm sure we'd have gone faster around the edges. But now -- in this I want to make sure the American people clearly understand this: Going fast does not take away the fact it still has to meet a court standard. So the issue is we're meeting a probable cause standard that still has to be reviewed by a court. And my argument is that's the wrong way to do this. We shouldn't be even going down that path.

REP. REYES: I understand.

MR. WAINSTEIN: Mr. Chairman, may I take a bat on that for a quick second?

REP. REYES: Sure.

MR. WAINSTEIN: I think that's a very important point, because people hear that we have this emergency authority and assume that, okay, then we can just sort of go up on it without any process at all. Keep in mind that under FISA -- under the emergency provisions of FISA -- the attorney general of the United States, and now with recent amendments to the statute delegated down to me -- we have to find that there is probable cause that the person we want to surveil overseas is an agent of a foreign power. And if we don't find that, we're not allowed under the statute to go ahead and authorize emergency authority. And within 72 hours we have to make that showing to the satisfaction of the FISA court. So it's a very important responsibility -- a weighty responsibility -- and it's nothing that we take lightly.

As a result, analysts -- whoever else is involved in process -- they have to pull together the information to establish that, to make that showing, and that can take some time in order to get that evidence together. And keep in mind, were it not for that -- if these surveillances overseas did not fall within FISA, we would not have to make a showing that the person that we want to surveil is connected to any particular foreign power, which is -- you know, our foreign intelligence, I mean, our foreign signal intelligence surveillances don't require that and they shouldn't -- for surveillances outside the United States they shouldn't fall within FISA. So it's very important that people understand the fact that we have emergency authority doesn't mean that we can automatically snap our fingers.

MR. McCONNELL: That's why my number one point always, Mr. Chairman, you know -- from the day I came back into active duty and looked at this -- my number one point was since I was on active duty before I never had to have a warrant for a foreign target in a foreign country and all of a sudden now I did because of where it was intercepted. That was the main thing I was trying to get people to recognize and deal with.

REP. REYES: I understood that you want to --

MR.       : (Off mike.)

REP. REYES: Ms. Eshoo.

REP. ANNA ESHOO (D-CA): Thank you for holding this public hearing, Mr. Chairman. I think it's so important because the American people are really worried about this. All one has to do is look at the editorials that were carried in newspapers in different parts of the country and the stated concerns about the bill that was passed.

Mr. Director, I want to ask you about a specific interview that was carried -- the chairman mentioned -- in the El Paso Times that ran on August 27th. You revealed a great of information that had previously been considered classified. I remember the discussion and the number being given to committee members and the -- I don't know whether the word warning, but it was certainly reinforced that this was a highly classified number.

So for example, you discussed the mechanics of the FISA applications and court review, including the recent changes in FISA case law that necessitated warrants for wire communications traversing our country. You also confirmed that -- you confirmed -- that private sector companies assisted in conducting the president's warrantless surveillance program.

Now my question on this is, did you discuss with the White House your intent to declassify these facts in advance of the interview?

MR. McCONNELL: No, I did not.

REP. ESHOO: And since you did not, why not?

MR. McCONNELL: The --

REP. ESHOO: How is this --

MR. McCONNELL: The control of classified information is subject to presidential authority, and the president delegates, on that authority, to me and it becomes a judgment call. So --

REP. ESHOO: So simply by stating in that interview with the El Paso Times, that the information just automatically became declassified because you stated it publicly?

MR. McCONNELL: It becomes a judgment call and -- I'll repeat some of the remarks I made earlier with regard to why I chose to do that. There were many claims and counterclaims. You opened your comments saying Americans are worried. Some were asserting, in those same editorials, that my community was conducting a drift net of surveillance --

REP. ESHOO: Well, I don't want to go back to what you've said before, and I appreciate your wanting to say more that was stated earlier today, but I only have a limited amount of time. I was really stunned when I read that, I have to tell you, and I think others were as well --

MR. McCONNELL: Ma'am, what I was attempting to do --

REP. ESHOO: -- I don't know, does it -- does the same thing occur if we, as members of committees, state a classified number and we decide that it should just be declassified? Or does that just come from DNI? (Cross talk.)

MR. McCONNELL: You would have to request authority to do that, and I have that authority, and I made a judgment. It was in my judgment call --

REP. ESHOO: Now were you aware --

(Cross talk.)

MR. McCONNELL: -- to provide for you and other members -

(Cross talk.)

REP. ESHOO: -- that by revealing the involvement --

(Cross talk.)

MR. McCONNELL: -- summary level information.

(Cross talk.)

REP. ESHOO: -- of private sector companies, that it undermined the Justice Department case, their defense against a lawsuit about the president's program?

MR. McCONNELL: I'm sorry, repeat the question.

REP. ESHOO: Well, when you confirmed -- confirmed -- that, I mean, there was a lot of speculation, but you confirmed that private sector telecommunications companies were assisting in the president's program. And I'm just asking you if you were aware if that undermined the Justice Department's defense against the lawsuit?

MR. McCONNELL: The words I chose was " private sector." And if you go back and closely examine all the articles that covered my interview, would quote me up to a point, and then it would stop the quotes and go on to name specific companies or telecommunications, or whatever, so.

REP. ESHOO: I think we -- I think we may view it differently, which is legitimate, but I don't -- I think it did some damage.

MR. McCONNELL: I just refer you back to the article which was -- which was printed verbatim.

REP. ESHOO: Yeah. After the Act passed, you claimed that because of the congressional and public debate over changes to FISA, quote, "some Americans are going to die."

MR. McCONNELL: Yes, ma'am, that's correct.

REP. ESHOO: Do you really believe that because we have a public debate in the Congress of the United States about surveillance, about the Foreign Intelligence Surveillance Act, that Americans are going to die?

MR. McCONNELL: Yes, ma'am, I do.

REP. ESHOO: And did Americans die --

MR. McCONNELL: They will.

REP. ESHOO: -- because of our debate?

MR. McCONNELL: They will. And the reason is this --

REP. ESHOO: I think you need to explain that, not just to us -- obviously the cameras are on. --

MR. McCONNELL: Intelligence business is --

REP. ESHOO: That's a -- that's a heavy statement.

MR. McCONNELL: Intelligence business is conducted in secret. It's conducted in secret for a reason.

REP. ESHOO: Did you ever advise the Congress not to debate this in public because you believe Americans were going to die?

MR. McCONNELL: I've been very clear about this all along. This is very important for us to get this right so we can do our mission to prevent Americans from dying, but --

REP. ESHOO: That's not what you said.

MR. McCONNELL: Well, if you'd allow me to finish, I'll tell you what I intended to say, and what I did say. If you compromise sources and methods -- and what this debate has allowed those who wish us harm to do, is to understand significantly more about how we were targeting their communications.

REP. ESHOO: Well, Mr. Director, with all due respect, I think that you put out classified information, and simply by stating so -- because you're director and you say that you have the ability to do that, that it just became declassified. I think that that was very important information that shouldn't have gone out, but that's only my judgment.

Now you're saying -- and standing by -- that, your previous statement that when we debate these issues in the Congress of the United States, which is our system, that Americans, some Americans, are going to die. And I really think that's a stretch. And I think, because of some of these things, it has done damage to what you bring forward. It puts a dent in the credibility, and I think that there are some members of Congress that are really affected by this. That's why I raise it.

REP. REYES: Ms. Wilson.

REP. WILSON: Thank you, Mr. Chairman.

Mr. Wainstein, would the Protect America Act allow the warrantless collection of an e-mail of a soldier communicating with his family back home?

MR. WAINSTEIN: Under certain circumstances it would, yes.

REP. WILSON: It would allow the warrantless collection of an e- mail of an American soldier overseas communicating with his family back home.

MR. WAINSTEIN: The Protect America Act allows us to target surveillance on persons overseas. Now keep in mind that one of the things that we have to do is we have to -- we have to satisfy the various elements of 105-B. And one of them is that the surveillance has to have a foreign, legitimate, significant foreign intelligence purpose. So we can't just target anybody just for kicks, the DNI and the AG have to say -- to certify that there's a foreign intelligence purpose for that surveillance.

Now keep in mind also, that this is an American soldier, that's a United States person. I think we alluded to this earlier, the director did, there is what's called the 2.5 process in place, which is 2.5 under the Executive Order 12333, which says that before we can target an American overseas for surveillance, the attorney general has to find that there's probable cause if the person is an agent of a foreign power. So he couldn't just target this agent -- this soldier just to get (regular ?) information.

REP. WILSON: The U.S. government would have to certify that there is probable cause to believe that that soldier overseas is an agent of a foreign power. Is that correct?

MR. WAINSTEIN: The attorney general would have to find that, yes.

REP. WILSON: Thank you. With respect to reversed targeting -- which is some concern of some folks, Mr. Wainstein, would it be -- would the Protect America Act allow a circumstance where you really want to listen to a doctor in America so you wiretap (that ?) relatives overseas. Would that be against the law?

MR. WAINSTEIN: It would be.

REP. WILSON: Thank you. Admiral, you testified in the Judiciary committee -- and it's already been discussed a little bit here, you said, "Let me give you an example. American soldiers captured in Iraq by insurgents, and we found ourselves in a position where we had to get a warrant to target the communications of the insurgents." In that circumstance, did you try to get an emergency FISA?

MR. McCONNELL: Yes, ma'am, we did.

REP. WILSON: How long did it take -- from the time the United States knew that it had a target, had some communication it wanted -- until you were able to get the attorney general to sign-off on an emergency FISA?

MR. McCONNELL: Ma'am, I have to get you an exact answer. What my memory serves, it's somewhere in the neighborhood of 12 hours or so. I don't remember for sure, but we'll get you an answer.

REP. WILSON: So it took, at a minimum of -- or about 12 hours to get the probable cause, to get it all the way through to get the signal to turn on the wiretap?

MR. McCONNELL: Yes, ma'am. And the point I was trying to highlight is just the fact of probable cause, and the standard that you meet has to be a probable cause standard that a court would approve -- that's the highlight.

REP. WILSON: But if that terrorist in Baghdad was using a push- to-talk phone, you could have gone up immediately?

MR. McCONNELL: That's correct. The reason was, the mode of communication, and where intercepted. That's what drove us to a FISA requirement -- or a warrant requirement.

REP. WILSON: So we had U.S. soldiers who were captured in Iraq by insurgents, and for the 12 hours immediately following their captures we weren't able to listen to their communications. Is that correct?

MR. McCONNELL: That's correct.

REP. WILSON: If it was your kid, is that good enough?

MR. McCONNELL: Ma'am, the reason I've tried to be as straightforward and open on this subject as I have -- because it is so important that we get this right.

Now many are going to accuse me of declassifying information -- warmonger, fearmonger, whatever, we got to get this right because sometimes those timelines are so tight. And that's what I meant by "the debate and the process could cost us American lives." We have to not extend 4th Amendment protection to a foreign terrorist, particularly in something like this where they're holding a U.S. hostage.

REP. WILSON: Mr. Wainstein, you're a Justice guy, you're familiar with kidnapping cases and the importance of things in this country like the Amber Alerts and the importance of those first hours in gathering information to protect American lives, often involving children. Was 12 hours good enough?

MR. WAINSTEIN: The point is, as the director said, that we need to be agile. We need to be able to jump and respond to circumstances immediately. This is a dangerous game, and whether it's this situation, or similar situations that happen every day, anything that slows down that process makes it more cumbersome, makes it more likely the terrorists will win.

REP. WILSON: Thank you. The threat persists. You both have testified to that fact, and that our laws did not, before the Protect America Act, work fast enough to protect this country against threats of people who are trying to create mass casualties against Americans. I thank you both for your work and I yield the balance of my time.

REP. REYES: Thank you, Ms. Wilson.

You know what I think? I think that if that is, in fact, the case that happened, I think that's an abhorrent failure of leadership on our part. And we shouldn't be worried about whether or not we're legally compliant when American lives are at stake, especially in a combat situation like that when you have the emergency provisions under the 72-hours guidelines --

REP. WILSON: Mr. Chairman.

REP. REYES: Ms. Wilson.

REP. WILSON: May I ask a question?

REP. REYES: Yeah, you may.

REP. WILSON: If they hadn't -- if they had not followed the law in that circumstance -- if they had said, forget the FISA, don't worry about the attorney general, just go up on that number and we'll worry about explaining later -- that they'd be breaking the law.

REP. REYES: The testimony that we've -- that we have had in committee by Mr. Jim Baker the other day is that all it takes is a phone call -- a phone call explaining the circumstances, a phone call explaining that American lives are at stake in a combat zone. I think it gets back to the bureaucracy and a failure, again, to recognize that American lives are at stake. I think -- I think it's a common sense thing to -- (inaudible) --

(Cross talk.)

MR. MCCONNEL: Mr. Chairman --

(Cross talk.)

REP. WILSON: That's why I supported the president --

(Cross talk.)

REP. REYES: That's why -- I think that's why the 72-hour emergency was --

MR. McCONNELL: Sir, the point that's maybe not being captured here is, even in an emergency, you still have to get approval. So someone has to say, yes, it's okay -- in accordance to the law. In this case, it's the attorney general. So the process to get the data, and put it in a format, and move it through the system, and get it approved --

REP. REYES: There were a number of other circumstances in this particular case, --

MR. McCONNELL: There were --

REP. REYES: -- but, again, I think -- I think it's imperative that we understand that there is that capability of making that phone call. I would be extremely surprised if the attorney general, or the acting attorney general, or the associate attorney general, once they got that call, they wouldn't say, "Go up on it. Let's make sure we're -- we're building a case," because all the elements were there that American soldiers' lives were in danger.

With that, Mr. Holt, you're recognized for five minutes.

REP. (     ?): Mr. Chairman, before you go to Mr. Holt, would you yield for a question to the chair on the issue that we're discussing regarding these soldiers that were -- that were captured. Could we get some clarification on why it took 12 hours? Was it a bureaucratic hold-up? Was it a legal hold-up? Or was it -- was it a technology hold-up? Given the testimony we heard from Mr. Baker yesterday, it seems ridiculous to me that it would take 12 hours to -- if we have identified a target, to be able to ascertain the information we need to protect the lives, or to find these soldiers that had -- that had been captured. I think there's a lot that's not being explained here.

REP. REYES: Well, we do have, and the committee does have the information, including the timeline and other circumstances that were involved, including the attorney general being out of -- out of town, and issues like that. But, again, it's available for any member of the committee. We do have it.

Well, I want to be careful not to divulge specific information that I may not be able to publicly, but we'll -- we're looking at that.

MR. WAINSTEIN: If I may, Mr. Chairman --

REP. REYES: Yes, Mr. -- (inaudible) --

MR. WAINSTEIN: -- very briefly, please. Thank you. I just don't want an impression to be left that wherever the attorney general was had, you know, is determinant -- determines when we get emergency authority. And I'm not going to talk about this particular case, it can be discussed in closed session.

But it must be understood that when we get emergency authority, the law requires that probable cause be shown. Probable cause that the -- the first one we want to target is an agent of a foreign power. And you don't have to go any farther than the discussion in the 9/11 Commission Report about the difficulties we had in establishing that showing from (Miscelli?) that took us so long to get authority to get a search warrant for -- to get authorization to search his laptop.

It's not an easy showing to make sometimes, and we have to make that showing. And I can tell you from experience that once we make it, it is almost instantaneous and it doesn't matter where the attorney general is, the call is made and he's responsive. But if we don't follow that procedure, we're violating the law and there are felony penalties that apply to violation of the law.

REP. HASTING: In this particular case, a common sense approach would have been: soldiers were kidnapped in Iraq; people were communicating among themselves in Iraq. Would that be foreign? Would that -- would that lead a common -- from a common sense perspective, a person to assume that probable cause was there?

MR. WAINSTEIN: Well, I'd have to divorce it from the facts here because getting into the facts gets into the -- a very sensitive area that we can't discuss, but I'd be happy to discuss it -- REP. REYES: Well, again, I don't want to leave the misperception that people were standing around because of FISA, unable to make a determination --

(MR. WAINSTEIN?): Mr. Chairman --

REP. REYES: -- There's a common sense --

(Cross talk.)

(MR. WAINSTEIN?): But that's -- (inaudible) -- Mr. Chairman.

(Cross talk.)

REP. REYES: -- every issue that we -- that we deal with, including FISA.

Yes, Mr. Hoekstra.

REP. HOEKSTRA: Thank you, Mr. Chairman. I mean, the commonsense approach to that is saying that FISA, probable cause does not extend to a foreign -- an agent of a foreign power, in a foreign country.

REP. REYES: That's exactly right. That's my point.

REP. HOEKSTRA: But in this case, because of the way the communications were routed, they got 4th Amendment protections and (some folks?) had to approve. --

REP. REYES: That's where -- that's where --

REP. HOEKSTRA: -- (inaudible) -- FISA.

REP. REYES: That's where I disagree with you because, again, American troops were kidnapped in Iraq; communication was taking place in Iraq -- the last time I checked, Iraq is foreign, you could assume that it's foreign to foreign in that case. I mean, I would find it astonishing if any judge would say that wasn't in compliance for emergency authority immediately.

MR. McCONNELL: Sir, the FISA Court said we would not be compliance. And that was the issue. I, sir, have briefed 260 members of Congress and I have just failed to make the point. The point is: someone in Iraq communicating; because it passed on a wire through this nation, this country, physically, the law said we had to have a warrant. That's the point. So what we're arguing is that we shouldn't have a warrant for a foreigner in a foreign country, regardless of where we intercept it. And that's -- that's what happened here.

REP. REYES: I don't think we have a disagreement on that. MR. McCONNELL: But we can't violate the law. We have to abide by the law. That was -- that was the whole point of the reason I brought it up. We're doing a consideration of probable cause for somebody in a foreign country because of where we intercepted it.

REP. REYES: Which was eliminated in 3356, at your request -- and which, I will tell you, we definitely need to make that --

MR. McCONNELL: Sir, I think -- I think everybody that I've talked to is in agreement with the first principle I keep putting on the table -- everybody. The issue with 3356, as we discussed, is when you add the other things, in some cases it put us back in the same situation.

That was the problem, we didn't have a chance to sit down across the table and say, what is your intent here and what's the probable outcome, and can how we pick a better word or a different word. That was our -- we got caught in a time crunch.

REP. REYES: Well, we're not in a time crunch now. We're -- we are going to be able to work with you, and I hope we cooperate --

MR. McCONNELL: Yes, sir, anytime, anywhere.

REP. REYES: -- for the good of our national security.

With that, Mr. Holt, you're recognized for five minutes.

REP. RUSH D. HOLT (D-NJ): Thank you, Mr. Chairman. Thank you for holding these public hearings.

Thank you both, gentlemen, for coming today.

I understand, Mr. Director, that you believe strongly that we need to change -- or the legislation needed to be changed so that there'd be no individualized judicial warrants required for overseas targets. Let me go through a few other things, though. Did you need and do you need the ability to conduct warrantless searches of Americans' homes inside the United States?

MR. McCONNELL: No.

REP. HOLT: Do you need or did you need the ability to conduct warrantless searches of domestic mail?

MR. McCONNELL: No.

REP. HOLT: Do you need to be able to conduct warrantless surveillance of U.S. persons whose communications might be about foreign intelligence?

MR. McCONNELL: Sir, ask the question again. Make sure I understood it.

REP. HOLT: Do you need to be able to conduct searches without juridical warrant of persons whose communications might be about foreign intelligence?

MR. McCONNELL: It depends on where and who the person is. If it's a U.S. person --

REP. HOLT: This is a U.S. person.

MR. McCONNELL: U.S. person in this country, it requires a warrant.

REP. HOLT: And not in this country? A U.S. -- a person protected under U.S. laws --

MR. McCONNELL: There is a --

REP. HOLT: -- and constitutional protections.

MR. McCONNELL: There's a situation there which -- is covered under Executive Order 12333. You have to have a authorization, but in the current interpretation that's not a warrant.

REP. HOLT: Not a warrant.

MR. McCONNELL: It's a ruling from the attorney general.

REP. HOLT: Do you need to be able to conduct warrantless searches of library records, medical records, business records under FISA?

MR. McCONNELL: Not to my knowledge.

REP. HOLT: Do you need to be able to conduct bulk collection of all communications originating overseas?

MR. McCONNELL: Bulk collection --

REP. HOLT: Collections.

MR. McCONNELL: -- of all communications originating overseas -- that would certainly be desirable if that was physically possible to do, since I'm in the foreign intelligence business.

REP. HOLT: Yeah.

Do you need to be able to collect -- or conduct bulk collection of communications from overseas to an American?

MR. McCONNELL: No.

REP. HOLT: Do you need to be able to conduct bulk collection of call detail records -- metadata for every domestic-to-domestic phone call by Americans?

MR. McCONNELL: Metadata is -- think of it as not content, but a --

REP. HOLT: That's right.

MR. McCONNELL: -- a process for how you would find something you might be looking for. Think of it as a road map. REP. HOLT: Yeah.

MR. McCONNELL: But without -- let me answer your question --

REP. HOLT: But with the exception of that one matter that -- yes, please. Go ahead.

MR. McCONNELL: Let me just answer your question. Should I do that without a court order? No.

REP. HOLT: Yeah, okay.

MR. McCONNELL: If I do it, I should have a court order if it's in this country.

REP. HOLT: So would you object to statute language that explicitly prohibits the government from engaging in these things?

MR. MCONNELL: The way we've discussed it in every case you've described, we are prohibited without a court order.

REP. HOLT: Yes. And so you would not object to explicit clarification of that in statute.

MR. McCONNELL: To go back to my dialogue with the chairman, as long as we examine the language with a team of experts to understand the consequences and the unintended consequences, I wouldn't object.

REP. HOLT: Yeah.

MR. McCONNELL: But what I couldn't do is agree to it without being allowed to read the text or have an expert team examine it, which was the situation back in July-August.

REP. HOLT: Yeah.

Now before the recess -- during negotiations over FISA modifications, you issued a statement saying that you strongly opposed the bill that was before Congress and insinuated that it would limit your ability to warn Americans of impending attacks. But later, you said you hadn't read it. Last week before the Senate Homeland Security and Government Affairs Committee, you said that under the new law you would lose, quote, "50 percent of our" -- without the new law, you would lose 50 percent of our ability to track, understand and know about these terrorists. This week, before the House Judiciary Committee, you said that if we let the new law expire, we would, quote, "lose about two-thirds of our capability and we would be losing steadily over time."

A week or so ago, you said that the new FISA law facilitated the recent disruption of the German terrorist plot despite the fact that this surveillance began many months before under old FISA authorities. You did, after the chairman and I and others made public statements -- you issued a public statement. But let me ask if you understand why some people have raised questions about the credibility of your arguments. Do you understand that there are some doubts about your ability to act as an unbiased source of information concerning this proposal -- these legislative proposals?

MR. McCONNELL: Sir, many of the quotes you've taken have context to them. They were answers to questions that were specifically framed. The question I received in the Senate hearing that you make reference to -- the question that I understood was, "Did the FISA process make any difference?" And my answer was, "Yes, it did." That was a key source of information. Once it became a political circus as to well, is it new law or the old law, the best thing for me to do was just to say, "I retract the statement. I'll clarify it in another hearing or in closed session." Did FISA make a difference and save American lives in Germany? Yes, it saved American lives. Did it matter if it was passed on the 5th of August or earlier? That wasn't my point. It was the FISA process. My point was it's 50 percent -- more than 50 percent of -- what we know about terrorists that are plotting to kill people in this country. And the way you framed your question was out of context for what I was trying to respond to in a -- either a hearing or to some question I was trying to be honest and straightforward about.

REP. HOLT: Well, later I will read the full transcript to you. But my time has expired.

I thank you.

REP. REYES: Thank you, Mr. Holt.

Mr. Issa?

REP. ISSA: Thank you, Mr. Chairman.

Tom (sp), would you take that down to the admiral?

While he's doing that, I just want to go over one thing on Title 50 U.S. Code Section 105(f), the Emergency Order Permission. I took the liberty of taking a quick glance at it, and I'll ask that it be included in the record at this point.

REP. REYES: Without objection.

REP. ISSA: Thank you. Thank you, Mr. Chairman.

It's straightforward. It says you can do this. Unfortunately, as I read it -- and I'd like your read on it and, obviously, the attorney general's office, too -- what we did when we structured this legislation is we made it simple -- said you can do it. But in the same 105, what we went on to do was endlessly tell you what you had to do after that -- within that 72 hours. And if I understand correctly, notwithstanding the chairman's statement that -- you know, you wouldn't wait 12 hours -- you wouldn't take 12 hours if it was your child, and you probably wouldn't. You'd be willing to go to jail, you'd be willing to violate the law, you'd be willing to ignore that to save your own child's life. But that's not the standard we hold people to in law enforcement.

We hold them to the standard that they are not. We take them off cases if it's their child.

MR. WAINSTEIN: Yes, sir.

REP. ISSA: As I read the statute, it's pretty clear that you have to have ready a good-faith belief that you're going to be able to -- after 72 hours -- present to the judge this -- another two-and-a- half pages of what-ifs and notwithstandings and so on. Is that correct, Admiral?

MR. McCONNELL: Yes, sir. That's correct. That's the point.

REP. ISSA: Okay.

So in a nutshell, what -- as we've talked past each other for the last 45 minutes, it's pretty clear that in Congress wanted you to have what General Petraeus has, which is they take our troops, he sends the gunship out, he kills the bad guys and gets our people back. If they wanted you to have that, they would give you 72 hours to take gunships out, so to speak without saying, "And -- oh, by the way, here's what has to be in your after-action for this to have been lawful." Is that right?

MR. McCONNELL: Yes, sir.

REP. ISSA: Okay.

I remember that -- and I think General Petraeus has been very good -- everybody who -- everybody who's been over there, as the ranking member has, I have, the chairman has -- General Petraeus explains that to us, that he can shoot somebody while they're calling the United States. He just can't listen to them while they're calling the United States.

MR. McCONNELL: Yes, sir.

REP. ISSA: Okay.

And I only put this into the record -- the Marine Online statement because I think it's important, notwithstanding the chairman's "We're not going to spy on our troops." I have checked and confirmed -- and you have in front of you -- which I also would ask to be put in the record anecdotally -- that every U.S. Department of Defense site both here and theater has a warning that says, "You may be monitored." As a matter of fact, it specifically makes it clear that you will be potentially monitored -- REP. REYES: Without objection.

REP. ISSA: And for Mr. Wainstein, I guess my question is your understanding of how the Uniform Code of Military Justice works. The -- when somebody's given a warning like this, when somebody's in theater, is it fair to say their Fourth Amendment is not in fact -- that in fact, if they do something inappropriate, including go to a porno site, they can -- this can -- that evidence can be used and they have no expectation of privacy. Is that right?

MR. McCONNELL: Yeah, sir, I don't actually have the -- (CD ?) past the Admiral, but Americans -- the 4th Amendment protections do follow Americans when they go overseas. But obviously, if you consent to -- you can see a banner that says like by using this you consent to us looking at it and possibly using it against you if you do something wrong. If that's what this banner says then yes, they've waived that.

REP. ISSA: Okay. Okay. And I only say that because we're not spying on our troops. Our troops are, in fact, consenting that for their safety that that happened. And I might --

MR. McCONNELL: And in addition, if I might say just --

REP. ISSA: Yes, please.

MR. McCONNELL: -- a few moments earlier, if we do surveil (sic) a soldier overseas as American, we have to establish to the Attorney General that that person's an agent of a foreign power.

REP. ISSA: Of course, if they become a target. I might, for the record, remind us all that it was insiders, not U.S. troops, but insiders who blew up our mess hall in Iraq. And, in fact, they had access or at least presence of computers and so on. I think -- I think today what we're hearing is we're hearing the majority say on a bill that they wrote, we didn't co-sponsor, they voted for and they sent to the president and the president signed, they're saying please don't let us hurt ourselves again and the American people.

And I would hope that they don't really mean it. My understanding of the Rocket Docket in Virginia, it's about 18 months. So I just want to have that in the record because I think 12 hours, when you know you're going to a court, that the question of speed is highly questionable.

Director, I do have one question for you that is pertinent for both sides of the aisle up here, and that is, all of us who not only receive classified briefings as we do, but who constantly look to the unclassified internet information related to areas of study, could not miss that the New York Times and everybody else on and off the internet, has been reporting, with some inconsistency, but reporting Israel's attack on Syrian sites. And yet, members of this committee, having inquired, have essentially been told we won't be briefed.

And as much as I want to support you, and I have supported your need to get what you need, I would hope today, in an open hearing that you would realize that many of us are frustrated that we do get selective information. And that when you declassified something in El Paso, I respect the fact that you did so -- what you thought were the right reasons. But I would hope that we could change the policy, starting today, about selectively handing us little bits of information to tie us up, while, in fact, critical information that is all ready leaking around in an inconsistent way can be brought to a committee that has to make decisions on whether or not our plans and preparations and our eyes are the ground are appropriate.

So if you could comment on that specifically, maintaining an unclassified -- and I'm not talking about the specific incident, but I am talking about the question of how you select answering our questions, including the Chairman's Ranking Member's request that seems to be forever waiting to find out and negotiated as to whether or not this Committee receives it.

MR. McCONNELL: Sir, first of all, a very important question. And let me just give you my personal view as it's -- the oversight process -- sunshine's a good thing and not a bad thing so oversight and sharing of information is appropriate and healthy. And that's my personal belief on how we engage. On this specific instance you're making reference to, I'd be happy to talk to you about that.

There are some -- there are information at the classified level that wouldn't be appropriate for me to discuss now. And there are varying levels of what you can do and not do by agreement between the executive branch and the Congress. And so I have to be respectful of that process. But given the opportunity to engage in dialogue and share information, I'm going to default to the sunshine position of making it available.

REP. ISSA: Okay. Mr. Chairman, I appreciate your indulgence on the time.

REP. REYES: All right. Mr. Tierney, I think we've got enough time to have Mr. Tierney go. Thank you.

REP. JOHN TIERNEY (D-MA): Thank you, Mr. Chairman. Mr. Director, I don't think there's been any disagreement from the beginning as to whether or not a warrant is needed for foreign communications between a person in a foreign country and another person in a foreign country non U.S. citizen. There is no warrant required. And many of us have argued consistently that FISA never required a warrant under those situations.

And I know there's been some disagreement on that and the interpretation. I'm going to just read the section of the bill that had been filed by the Democrats last session that deals with the issue of whether or not -- clarifying that matter. I don't want you to respond now, but I would like you to submit to us after the hearing your complete reason why you thought that the following language wasn't clear enough to satisfy your needs to make it certain that no foreign communications required a warrant. Section 105(a) reads: Notwithstanding any other provision of this Act, a court order is not required for the acquisition of the contents of any communication between persons that are not located within the United States for the purpose of collecting foreign intelligence information without respect to whether the communication passes through the United States or the surveillance device is located within the United States.

So if you would be kind enough to just submit to us why you think that's not clear with respect to that issue, I would appreciate it.

Secondly, I think, Mr. Director, you would agree with me, and I think you stated pretty clearly here, Americans and others inside the United States do enjoy a constitutional protection, a right against unreasonable search and seizure or interception of their conversations, is that correct?

MR. McCONNELL: Right.

REP. TIERNEY: And it would be unlawful to intercept that communication without a warrant, is that correct?

MR. McCONNELL: Yes.

REP. TIERNEY: Then I assume that you agree with me that the original program that the president was operating was, in fact, unlawful.

MR. McCONNELL: Sir, that was a debate between the interpretation of Article II and Article I. Some would argue it's lawful. Some would say no.

But I can't resolve a Constitutional debate. I'm talking about the framework of FISA.

REP. TIERNEY: Well, moving it forward, we agree that if the government targets an overseas person, a certain percentage of foreign intelligence targets overseas will communicate only with other foreigners overseas. I think that's fair to say, right?

But some of them are going to communicate with individuals in the United States. And some of them -- of those communications are going to pass through the United States. And it may not, at first, be easy to determine if they are being routed to U.S. persons or to foreigners overseas. I think that's the crux of the government's dilemma here, is that right?

MR. McCONNELL: That's part of it, yes, sir.

REP. TIERNEY: Okay, now the government's been arguing for the agility and speed, and says it should not need to prepare applications for particularized orders, meaning specific persons or the specific thing to be intercepted, for foreign targets overseas. And that's the issue I think these laws have been trying to deal with. Still, you would agree with me I think, that when the government listens to both ends of a communication, one in the United States, as it admits it has done, and probably will do, even if inadvertently in the future, it does infringe on the privacy rights of Americans. And the question is whether or not that infringement is reasonable.

MR. McCONNELL: Sir, the issue for us is that you can only target one end of a conversation.

REP. TIERNEY: Right.

MR. McCONNELL: You can't control who that person might talk to.

REP. TIERNEY: Exactly. So for this purpose, the government has put in some selection filtering methods.

MR. McCONNELL: The issue is who you target.

REP. TIERNEY: Right.

MR. McCONNELL: If it's foreign or --

REP. TIERNEY: Well, the issue is -- the issue is not who you target because we all ready discussed that. You're going to target foreigners overseas. But sometimes they're going to have communications that have to go through the United States or that are with persons in the United States. So the issue is what are you intercepting?

MR. McCONNELL: That's correct. And the old law was that if it touched wire here, we had to have a warrant --

REP. TIERNEY: Well --

MR. McCONNELL: -- against the foreign target. That was the issue.

REP. TIERNEY: The issue for some. But Mr. Baker, who I think you'll agree with me is an expert on the legislation and implementation of FISA, at least your General Counsel, Ben Powell, said he was an expert in front of the Judiciary Committee --

MR. McCONNELL: He is an expert.

REP. TIERNEY: -- that he is an expert. He indicates to us in his testimony that it wasn't a situation of technology that really was the issue here. And he says that contrary to the history we heard earlier and his disagreement on that, that Congress anticipated the fiber optics and cable usage in overseas conversations when it did FISA back in 1978. But the real issue is who's the decision maker for authorizing what the selection should be? What justification should be required, and what standard of review the decision maker should apply? How individualized authorizations to conduct surveillance should be? And what role judges should play in this process?

He had testified that in many situations over the years, aggressive and well meaning attorneys throughout the government pushed aggressive interpretations of the law. But the question is to make sure we balance this with reasonableness. The government has these selection and filtering methods.

The question is whether that -- the government's criteria for determining selections and filters result in methods that are likely to ensure that communications that are being intercepted are to or from non U.S. persons overseas, and whether those communications contain foreign intelligence.

Now even that is backing off of the requirement that it be a foreign agent, or an agent of a foreign power; it broadens it out.

But assuming we're going that far on that, these standards are loosened. It's probably more important that we have adequate protections. Is there any reason why that determination of reasonable is whether or not those filtering methods are reasonable, shouldn't be left to a court as opposed to you, sir, as a DNI and the Attorney General.

MR. McCONNELL: Sir, they are -- under the law signed in August they are subjected to a court review.

REP. TIERNEY: Well, after the fact.

MR. McCONNELL: Well --

REP. TIERNEY: Significantly after the fact, and then only to a standard of clearly erroneous. Which basically means they have to give incredible deference to the administration; not just the usual deference. Is there any reason in your mind why, you know, that could not be subjected to judicial review at a reasonable standard, as opposed to clearly erroneous?

MR. McCONNELL: The issue I would object to is submitting it to the court before we can engage in conducting our mission.

REP. TIERNEY: Well, you're already engaged in your mission right now. So if we were going to create a law that would go into effect at a future date, is there any reason why that law to go into a future date, under that system, the judge could not first determine whether or not those selection and filtering processes were reasonable?

MR. McCONNELL: I would object to having a court be between us conducting the mission and giving us permission in the way you've describe it in a foreign person -- foreign country. Where it is now, the court will review it, as you mentioned, after the fact of procedures to make sure we're doing it right; we're not violating the law and --

REP. TIERNEY: Well let's back up. Let's have the procedures approved before it goes -- they go into effect.

MR. McCONNELL: And then you'll get us in the situation where we were discussing earlier where getting the emergency procedure for -- REP. TIERNEY: But you already have a law in effect right now, all right.

MR. McCONNELL: I -- wait, we have a law in effect which changed the hypothetical you're setting up. It wasn't the -- the FISA.

REP. TIERNEY: I'm talking about going forward, all right? But you have a law in effect and you are collecting now.

MR. McCONNELL: That's correct.

REP. TIERNEY: All right. So, if going forward, is there any reason why a court couldn't review for future use whether or not your methods are, in fact, reasonable?

MR. McCONNELL: The -- what we're targeting changes all of the time. So if you put the court between us and the foreign targets then that --

REP. TIERNEY: We're putting the court that's in a determination of whether or not your selection and filtering methods are reasonable.

MR. McCONNELL: Which is in law now.

REP. TIERNEY: Only --

(Cross talk)

REP. TIERNEY: -- it's not reasonable. The standard is clearly erroneous; whether or not your determination was clearly erroneous, which is an entire new standard for matters of 4th Amendment rights.

MR. WAINSTEIN: May I make a quick point on that, sir?

REP. TIERNEY: If I could get the Director's answer to that first, please.

MR. McCONNELL: Sir, what we tried to accomplish was having the court look at the procedures in a reasonable way. So that was what the --

REP. TIERNEY: But why did you accomplish not allowing the court to make a determination as to the reasonableness of those selections and filters?

MR. McCONNELL: I'm not objecting to that, so long as it's not in advance because our world is very dynamic. So I can't --

REP. TIERNEY: So you have no objection to the court making the review as to whether or not your selection and filtering methods are reasonable? MR. McCONNELL: Are reasonable.

REP. TIERNEY: That's fine. All right.

MR. WAINSTEIN: If I may, sir, just very briefly. The law that you passed requires that. But the standard, as you pointed out, as clearly erroneous. And you said that that's a new standard, it actually is -- that standard is actually in FISA, the original FISA.

REP. TIERNEY: Right, but not in this application, not with respect to whether or not you're looking at these selection and filtering methods. The clearly erroneous standard is a significant departure downward from the Fourth Amendment requirement that searches and warrants be based on reasonableness.

MR. WAINSTEIN: Sure, it's a different animal but, of course, this --

REP. TIERNEY: No, we're not talking about a different animal. We're talking about interception of communications of people in this country who are U.S. citizens. And so the reasonable standard -- there's no reason, as I understand it, and as the director is now saying he has no objection either, that the court look at the for the purposes of reasonableness.

Mr. Director, do you have any objection to the court actually looking afterwards at the reasonableness of the mitigation aspects that are put in play?

MR. McCONNELL: A review after the fact, no, as long as it doesn't interfere with our dynamic nature of our --

REP. TIERNEY: And do you have any objection to the Inspector General auditing the performance of the government under this law, or whatever law that might come along, so that it can report to Congress on what has transpired under the act?

MR. McCONNELL: The -- I'd have to understand exactly what that means. There are about four levels of review now. So --

REP. TIERNEY: We've got all -- all the hens watching the -- the -- the fox watching the henhouse.

SEN. REYES: If I can interrupt just -- we've got three votes. We're going to have to recess. You're certainly welcome to come back.

REP. TIERNEY: Let me just ask this one question and I'll be done.

REP. REYES: Okay, one -- one last question.

REP. TIERNEY: That is, you know, do you have any objection to the Inspector General's Office doing a review and reporting to Congress on the implementation of this law?

MR. McCONNELL: If it was something requested by the Congress as a part of the Congress' duties, that's something you could request. But I think the standard we have now established is sufficient because there are four levels of review.

REP. TIERNEY: What's standard right now is that the executive will watch over the executive and report about what the executive is doing.

MR. McCONNELL: No sir, it involves the court and it involves the Congress.

REP. TIERNEY: Well, we can have the discussion as the Chairman wants to leave. But it does not, in any semblance, of a satisfactory manner in my view. Thank you.

REP. REYES: Thank you. We have three votes. We're going to recess. We should be back in about 20, 25 minutes. Committee stands in recess.

(Recess.)

REP. REYES: The committee will please come to order. The next speaker will be Mr. Ruppersberger, recognized for five minutes.

REP. C. A. DUTCH RUPPERSBERGER (D-MD): Mr. Director, first, I think that this is an issue that we should come together -- Republicans, Democrat, as a country and that's why we're having these hearings. We know we were rushed through but we do need to resolve some of these issues. There's no question that everyone here is going to give the tools pursuant to our constitution to be able to fight terrorism.

But, you know, I think the big issue and the big dispute is the issue of oversight. Our forefathers created a great system of government with checks and balances and we need to continue those checks and balances as it relates to Americans. That's what our men and women in the military fight for, for our freedom and liberty, and also our constitution. Now, Director McConnell, I'd like to ask you three issues. I said -- you said that you needed three components to deal with what we have. Number one, no individual warrant for foreign targets. Would you agree?

MR. McCONNELL: Mm hmm.

REP. RUPPERSBERGER: A way to compel the private sector to assist surveillance.

MR. McCONNELL: With liability protection.

REP. RUPPERSBERGER: And three, a requirement for individual warrants when targeting Americans.

MR. McCONNELL: A U.S. person -- yes, sir.

REP. RUPPERSBERGER: Yes, a U.S. person, not foreign. I think it's very clear in the old law what we're talking about now -- that we don't need a warrant as it relates to foreigners.

MR. McCONNELL: Sir, a U.S. person could be a foreigner if he's in this country. Even they get -- a U.S. person and foreign -- even a terror suspect would get that protection if he's in the United States.

REP. RUPPERSBERGER: Well, that's up to interpretation, and we need to clarify these laws and that's what we're here to write the laws, and right now I think just the president's statement yesterday there's no clarity. I happen to represent the district where NSA is located, and I'm chairing the committee that oversees NSA. So a lot of the people working at NSA are my constituents, and they need clarity. They need to go to work every day and know what is right, is wrong, and not have to worry about these issues.

MR. McCONNELL: Fully agree -- fully agree.

REP. RUPPERSBERGER: Now, the -- with the three components you just agreed to it's my belief that the negotiations that we had in the Democratic bill of H.R. 3356 addressed all these issues. Do you feel that they did or did not address these issues?

MR. McCONNELL: No, sir, not when you extend some of the language as to the impact, and that was our issue.

REP. RUPPERSBERGER: All right. Well, let me ask you this. I believe from what I've heard today that we are very close to resolving the issue. The one point is the oversight and, you know, I can say this. This issue that has been used about Iraq and Americans kidnapped -- that is a leadership -- that's a command issue. We -- this law will allow us to react at any time. All -- and all we're doing, and I think people are -- misunderstand the fact that there's so much volume that has to be done in these very rare circumstances and we -- the testimony that we have clearly has persuaded me that we in no way need to have even probable cause if it's an emergency situation that exists, and you can act upon that and you need -- you can act upon that. However, you have the 72 hours to develop so the court oversees it, but the court is only overseeing process, not each individual case. Would you agree with that?

MR. McCONNELL: Sir, in the old law we had to have probable cause that would stand up. Under the new law, which was signed in August, we do not -- we would not have to have now a warrant foreign person, foreign country. That situation wouldn't arise again in the current law.

REP. RUPPERSBERGER: And yet, we have no judicial oversight and that is where the issue -- that's not what our -- that's not the system our forefathers created. Let me go further. You have said that you agree that the court should be involved reviewing procedures for surveillance that may involve Americans after the surveillance begins, correct?

MR. McCONNELL: I'm sorry -- couldn't quite hear --

REP. RUPPERSBERGER: You have said that you agree that the court should be involved in reviewing procedures for surveillance that may involve Americans after the surveillance has begun.

MR. McCONNELL: No, sir, not exactly. The current -- the law says currently if it involves U.S. persons we get a warrant so that's a decision up front that now -- the -- I think what you're describing is the law now subjects to the court review of our process and procedures to make sure it's consistent with the law. I agree with that. REP. RUPPERSBERGER: You agree with that? Well, let me get to one other area. My time's starting to run out. Wiretaps -- I used to do wiretaps as an investigative prosecutor always with the courts. Dealt with the telecom companies. You can't have wiretaps if you don't have their support and they need to work with you. And I agree that there should be some type of immunity as it relates to the telecom companies because they're really acting on behalf of their nation as really an agent of the United States.

But here's a problem that we have. To just say you want immunity is not enough. We want to know what we're giving immunity for, and unless we get the documents that we've asked for it's just -- I can't understand why there's resistance to give us the information that we want to see from the administration, and if we get that I believe that we might be able to come together and to put together a bill very quickly on behalf of our country and give our -- the resources that we need to deal with the issue of terrorism. Now, please address the issue of why we have not been able to receive this information. We cannot give blanket immunity to you until we find out what we're giving immunity for. Would you please answer that?

MR. McCONNELL: Sir, all I can say is it's not something I'm responsible for. I've made my recommendations. It's a subject under current dialogue between the various committees.

REP. RUPPERSBERGER: Did you make recommendations to the administration that -- to give us information so that we can make a decision on the immunity?

MR. McCONNELL: My recommendation is to give the Congress access to what they need for the oversight purpose.

REP. RUPPERSBERGER: And will you continue to be very strong in your recommendations to the president in that regard?

MR. McCONNELL: That's -- I'm strong in that because I believe it.

REP. RUPPERSBERGER: Well, if you do I believe that if we can see that then we might be able to resolve this entire issue without the anxiety and the president going to NSA and talking about lives at risk. We're going to -- we all care about American lives and we will do what we have to do to protect them. Thank you.

REP. REYES: Thank you, Mr. Ruppersberger. Miss Schakowsky?

REP. JAN SCHAKOWSKY (D-IL): Thank you, Mr. Chairman. Director McConnell, I'm wondering, first, if you would provide to the committee in classified form specific instances of how NSA or the intelligence community was prevented altogether from collecting foreign intelligence prior to the passage of the PAA. You say those words, prevented altogether, on Page 6. Mr. Wainstein says prevented altogether on Page 5 of his testimony. And so I'd like to know how the law prevented altogether in which instances you were prevented from the ability to collect foreign intelligence, and I'd also like to know in your -- when you present that to the committee in classified form how H.R. 3356 did or did not correct that problem. That's a request. Would you comply with that request?

MR. McCONNELL: Yes, ma'am.

MR. WAINSTEIN: I -- (inaudible) -- answer that right now if you'd like. Would you like to answer that?

REP. SCHAKOWSKY: Well, I'm -- I would imagine that there are specific instances that you would want in classified session but if you want to briefly answer that.

MR. WAINSTEIN: Just generally, I think it's important to note that one of the things that is required when we have to go through the FISA court is we have to show probably cause that the person we want to target is an agent of a foreign power, and in the rest of our -- (inaudible) -- intelligence collection we don't have to do that. That's a big burden. That's a --

REP. SCHAKOWSKY: No, I want to -- but I would like to know -- and that's why I would prefer to have it in a classified form because I want to know the times that you were prevented from doing that. But let me go on --

MR. WAINSTEIN: I understand, but in the abstract it's -- you can understand that there are a number of instances where we cannot make that showing and we could therefore not do that surveillance, and that is one of the issues I think that we had with the bill.

REP. SCHAKOWSKY: I want to assure myself by seeing those instances. Director McConnell, we've been repeatedly told that the rights of U.S. persons would be protected under the new authorities because the NSA would minimize.

You talked about minimization -- U.S. person information. So will you commit that you will be able to tell us how frequently U.S. person information gets collected under the new act?

MR. McCONNELL: We'll -- we will look at the information -- see what can be made available. As I tried to explain on a similar question earlier, we may not be able to even answer the question, but what we can find we'll provide to the committee.

REP. SCHAKOWSKY: Well, okay. Then -- and will you be able to -- will you commit to -- that you'll be able to tell us how many times U.S. person information gets disseminated under the new act?

MR. McCONNELL: Yes, ma'am. That's an easier thing to do.

REP. SCHAKOWSKY: And will you commit that you will be able to tell us how many times information gathered under the new act gets used to seek FISA warrants against U.S. persons?

MR. McCONNELL: That would be a relatively straightforward thing, yes.

REP. SCHAKOWSKY: Okay. So you may not be able to tell us how frequently U.S. person information gets collected under the new act. If you're unable to answer that basic question, how is this committee going to be able to do proper oversight to exercise our constitutional mandate to do that kind of oversight to protect the rights of Americans?

MR. McCONNELL: Well, ma'am, as I tried to explain earlier it may be incidental question -- incident collection. You don't -- there's no human that is aware of it so you wouldn't know that until you went into the database. That's why I was saying to answer your question specifically it may not be an answer we can get. Now, once there's some reason to look at data then we can -- we keep track of that. We'd certainly be happy to provide it to you.

REP. SCHAKOWSKY: Okay, but so the -- so there may be information about Americans in that database. I'm looking at your testimony before the judiciary committee on Monday -- "I'm not even sure we keep information in that form. It will probably take us some time to get the answer." And then later you say, "It might create a situation where it creates significantly extra effort on our part." I think the protection of the privacy rights of U.S. Americans is worth effort. I mean, I -- if names are in a database and they're sitting in a database of innocent Americans it would seem to me that that would be something this committee -- that this Congress should be able to have oversight on.

MR. McCONNELL: Well, ma'am, let me try to put it in a context -- maybe use an example where it would make -- little easier to understand. There are literally billions of transactions, and remember, the mission is foreign intelligence.

REP. SCHAKOWSKY: But how do you know it's incidental if you don't have the statistics?

MR. McCONNELL: In the context of foreign intelligence we can't control what foreigners might say about Americans. Frequently, there's a reference to a political figure in the United States or something. We may not know that's in the database until we had some reason to go query that portion of the database for a foreign intelligence purpose, so it could be there and us not be aware of it. That's the point I'm trying to highlight. Where it's -- where it has been used or specifically excluded from the database we probably can provide those numbers. I just don't know the extent of it but I'll be happy to look at it and see what we can provide to you.

REP. SCHAKOWSKY: You know, Mr. Chairman, let me just say that on a number of occasions we have found that databases have collected private information about American citizens, and later on then -- well, we made a mistake -- it shouldn't be there -- we should get it out of the database. I would prefer to see that at the beginning of the process -- that we make sure that we protect people's rights and that that become a priority regardless of the effort that it may take. Thank you, Mr. Chairman.

REP. REYES: I thank the gentlewoman. We'll pursue that from a committee standpoint. Mr. Langevin?

REP. JIM LANGEVIN (D-RI): Thank you, Mr. Chairman, and gentlemen, thank you for your testimony here today. I appreciate the difficult job that you have on your hands and all that you're trying to do to protect the American people. We are in this together and we want to make sure, of course, that you have the tools that you need in order to protect the country. Equally important, we want to make sure that we are protecting the rights -- the civil liberties -- of the American people, and that's what this struggle really is all about and what is the right balance. And I think we're all on the same page. We're very, very close on most of these issues. We clearly -- there's unanimous agreement here that we don't need a warrant for foreign-to-foreign communications, and I want to make that clear for those that are watching. I did want to get into some of the questions with respect to surveillance of, you know, insurgents and the example in Iraq had been given. Correct me if I'm wrong but, you know, insurgent by its very definition would qualify as an agent of a foreign power. So when you're talking about, you know, justification for probable cause that is your probable cause, right? I mean, it's --

MR. McCONNELL: Yes, sir. It's just the process of going through that and submitting it to the court is the issue.

REP. LANGEVIN: But it's -- you don't have to -- it's not a heavy lift to prove that that's a --

MR. McCONNELL: No. My point is that it just took -- it took time and then it had to satisfy a court for a probable cause standard. That was what I was trying to highlight.

REP. LANGEVIN: Yeah. And I also -- I want to get into the, you know, the process part of this is that one thing we really haven't drilled down into is the fact that the process really -- there's really two parts of it. There is the legal or management or judicial part of the process, and then there's the technical part of the process.

And clearly either before the Protect America Act was passed or after, although it clarifies and as did the House bill that we passed that those pretty much -- we believe that it satisfied all the three requirements that you said that you needed and we bent over backwards to try to make sure that we gave you what you needed in terms of being able to conduct proper surveillancing and at the same time protecting civil liberties, that House-passed bill solved the management and the judicial part of it. But the reality is even the Protect America Act did nothing to change the technical aspects or the steps that needed to happen physically in order to do surveillance.

MR. McCONNELL: It took away the requirements for probable cause. That was the main change.

REP. LANGEVIN: That is a management change. That is the judicial change. But --

MR. McCONNELL: That's the -- that was the --

REP. LANGEVIN: -- we talk about the delay and the --

MR. McCONNELL: That was the requirement in the law. That was what I'm trying --

REP. LANGEVIN: -- even in surveillance it's -- there is still technical things that happened that take time.

MR. McCONNELL: Yes, sir. No question. I mean, that's not automatic -- right. REP. LANGEVIN: So I wanted to, you know, the Protect America Act -- even that went only so far. I mean, there were certain, you know --

MR. McCONNELL: Still going to take some time -- no question.

REP. LANGEVIN: Right. So I want to clarify that for the American people -- for those that are watching. Let me while my time -- while I still have my time, Director McConnell, on September 17th, this committee had received a letter from -- actually let me go into another area because I would -- I don't have that much time left.

You had made various statements sometimes that seemed to be inconsistent in the whole process when we were deciding between the administration's bill and comparing that with the -- with 3356, the Reyes-Conyers bill. For example, on August 3rd, 2007 on the eve of the House vote -- H.R. 3356 -- you issued a statement claiming that the House proposal was unacceptable and that the bill would not allow you to carry out your responsibilities to provide a warning to protect the nation.

Yet during a recent interview with the El Paso Times you had noted that you never had a chance to read the bill because, again, it was so complex. Can you clarify which of those statements are accurate? And I'm looking at your -- the statement that you had on the website and I can read it if you need to but can you clarify for --

MR. McCONNELL: Sure. I'd be happy to, sir.

There were -- in the final flurry there were seven bills exchanged, I think four from the administration and three from the Congress, or vice versa, I don't remember. So what I might have been referring to was -- was the situation in the Senate.

When -- what we were facing in the last few moments was very senior people calling me, say, do you agree to these points? What I was trying to go back to were the three philosophical points or fundamental issues you had highlighted earlier, which is my point of view.

I had a team of 20 or so lawyers that are technical experts in aspects of it. So once we had examined the House bill, there were portions of it that inserted ambiguity. And you just -- you slipped into it a moment ago, you said foreign to foreign. Many people would like to say, it's okay if it's foreign to foreign. And what I keep trying to highlight for the committee is, you can only target one thing. You have no control over who the person at the other end of the phone is going to call, or who is going to call that person.

So the language that was in 3356, inserted ambiguity and uncertainty, but weren't sure that it would come out the way we needed it to come out to do what we thought to protect the nation.

REP. LANGEVIN: Did you in fact read the House-passed bill?

MR. McCONNELL: I personally skimmed it over, did not read it in infinite detail. As I said I have a team of 20 lawyers that knows every piece of it, were examining the intended and unintended consequences. So any statement that I issued would have been a result of that process.

REP. LANGEVIN: I just wanted to point out that both the House- passed bill and the administration's bill were each six pages long, so it's not a heavy lift to read through it thoroughly.

MR. McCONNELL: I understand that, sir. But let me just highlight the definition of electronic surveillance. What we were attempting to do was to get foreign target, foreign country, excluded from that definition. If you don't exclude it then it has consequences throughout.

REP. LANGEVIN: And director, my time is expired, but I just wanted to clarify that clearly my opinion, both then and now, is that's exactly what the House bill did, gave you the things that you needed to do to exclude foreign and foreign, it was not an issue.

MR. McCONNELL: Be happy to sit down and go through it to let you see our point of view, and your point of view, and see if we can't agree on some language that's what we both agree on.

REP. LANGEVIN: Well, I hope we can do that.

MR. McCONNELL: Yes, sir.

REP. LANGEVIN: Thank you, Mr. Chairman, and I yield back.

REP. REYES: Thank you, Mr. Langevin.

Ms. Wilson.

REP. HEATHER WILSON (R-NM): Thank you, Mr. Chairman.

There's been some discussion here about using our using commonsense, and that particularly in cases of emergency people should use commonsense and that we should listen to people overseas, particularly in a case where somebody has kidnapped our soldiers.

Mr. Wainstein, is there a commonsense exception to the requirements under FISA?

MR. WAINSTEIN: No, ma'am, the requirements are pretty stark and clear, and there are criminal penalties if you violate them.

REP. WILSON: So if our -- if someone said, look, this is -- this is an emergency, we are all reasonable people here, we know we've got to find these guys, let's go up on the number, and we'll -- we'll take care of the paperwork later. Would that be a felony?

MR. WAINSTEIN: It would be.

REP. WILSON: Are you willing to commit a felony?

MR. WAINSTEIN: No, as a -- as a public servant I cannot violate the law, though I understand the thought that it would be nice under those circumstances to do whatever is necessary to save American lives, the reality is that we can't do that.

REP. WILSON: In a case where you've got an analyst forward who perhaps located in Baghdad, who thinks that he has something, things he has something that might be able to help in an emergency situation, knows it's an emergency situation. Can he pick up the phone and call you and say, hey, Ken, I've got something here that's really important. This is why I think that. Can you sign off on it? Can that in reality happen? MR. WAINSTEIN: It does happen. These calls go straight into the folks who work directly with me. They'd get right to me and get right to the attorney general. That actually happens in very short time.

The problem is, they have to have the information necessary to satisfy the probable cause standard.

REP. WILSON: So they have to be able to show you that they have probable cause to believe that this guy in a foreign country is affiliated with a foreign power and so on and so forth, all the requirements that are set out in the statute?

MR. WAINSTEIN: Exactly, and if I could play this out, if we go ahead and authorize emergency -- grant emergency authorization to go ahead and go up on surveillance, and within 72 hours we are not able to satisfy the probable cause standard to the FISA court that surveillance goes down, we lose that surveillance.  But also there are penalties in the statute that we then -- there is a presumption we'd have to actually notify the target that we had been surveilling them, which as you can imagine, creates problems.

REP. WILSON:  Wait a minute, let me make sure I understand this. So if we move too fast, we didn't meet the probable cause standard for a foreign person in a foreign country who is probably an insurgent, and the FISA court here in Washington says, no, you didn't meet that probable cause standard, we would actually have to go out and find the insurgent and tell them that we were trying to listen to them?

MR. WAINSTEIN:  In theory, we would, yes.  There is a presumption that we actually notify the target of the fact of the surveillance, which as you can imagine would really compromise our intelligence operations.

So it's a -- because of that, and just because we have to adhere to the law, we take that responsibility very seriously to make sure we have sufficient evidence; no more than bare sufficiency, but we have sufficient evidence to satisfy probable cause.

REP. WILSON:  And the Protect America Act fixes this problem?

MR. WAINSTEIN:  Yes, for targeting people overseas, it does.

REP. WILSON:  When was this committee first briefed on the particular case that we've been talking about?  Do either of you remember?

MR. McCONNELL:  Ma'am, I can get back to you, I just don't remember. It was actually briefed to you by another group in our community, and I don't remember  the exact date.

REP. WILSON:  Do you remember about when?

MR. McCONNELL:  I'd say probably May -- our pool back here says we think it was May, but we will get you the specific date.  REP. WILSON:  I believe you correct.

I want to thank both of you gentlemen for your work on behalf of this country.

I would ask one final question.  Under the statute the attorney general is required to report on all electronic surveillance in the United States conducted under the Foreign Intelligence Surveillance Act as amended every six months to this committee.

Will you provide that information, and will you continue to provide that information to the committee as required by law, Mr. Wainstein?

MR. WAINSTEIN:  Yes, absolutely, and we will also do the additional reporting that we've agreed to do in regard to the Protect America Act.

REP. WILSON:  And can I continue to go out to the National Security Agency as I have before and be given open access to all of their cases with respect to satisfying for myself that -- that you are following the law?

MR. WAINSTEIN:  Absolutely.

MR. McCONNELL: Yes, ma'am.

REP. WILSON: Thank you, Mr. Chairman.

MR. WAINSTEIN: If I may, Mr. Chairman, just briefly correct one thing. When I told you about that -- the provision that says we have to notify the target if we go up on emergency authorization and don't end up getting court authorization.

That requirement is actually limited to U.S. persons, so let's say we have a U.S. person who is an agent of a foreign power. We go up on that person overseas. We'd have to notify him just because I think the hypothetical you posited was an insurgent, in case it's not a U.S. person insurgent, we wouldn't have to.

REP. WILSON: But in the case of whether -- if it was a U.S. person overseas that we were tracking, and we went up too quickly?

MR. WAINSTEIN: Yes, we'd have to. And not only does that have practical consequences, but it reflects the seriousness with which Congress and the court takes our assessment of the evidence at the front end to make sure that there's probable cause.

REP. WILSON: Thank you very much, Mr. Chairman.

REP. REYES: Thank you, Ms. Wilson. And thank you for clearing that up, because I was going to ask you that very same question.

MR. WAINSTEIN: Thank you, sir.

REP. REYES: Mr. Holt.

REP. HOLT: Thank you, Mr. Chairman.

Mr. Director, you said that emergency provisions under FISA still have to meet a probable cause standard.

MR. McCONNELL: It did earlier, not now.

REP. HOLT: But not now? So what standard do they have to meet? Is it the hunch of a political appointee? Is it the firm belief of a dedicated professional in the middle of the administrative chain? Who has the responsibility then for determining that -- it is not a probable cause standard. What standard is it, and who applies that standard?

MR. McCONNELL: For a foreign target in a foreign country, is that the question?

REP. HOLT: The standard that justifies intercepting and storing and maybe in the future analyzing a communication.

MR. McCONNELL: For a foreign target in a foreign country?

REP. HOLT: For any of that, whose determining whether it is a foreign target. Who is determining whether this is someone whose conversations should be intercepted?

MR. McCONNELL: Well, since our mission is foreign intelligence, the standard would be enforced by the analyst working the problem against a foreign target in a foreign country.

REP. HOLT: And if this person who is responsible for it knows that there is no judicial oversight, not in 72 hours, not ever, do you think this person will make the decision differently under this law than the person would have made it under, say, FISA?

MR. McCONNELL: No, I don't think so.

REP. HOLT: Okay. So the FISA law would have been just fine because operationally the person wouldn't make the decision any differently under this law, I believe I just heard you say.

MR. McCONNELL: That's not correct, sir. I'd like to respond to that.

REP. HOLT: All right.

MR. McCONNELL: The issue we're discussing is, do you have to have probable cause submitted through an approval process for a court on a foreign person or foreign country? That's what we're trying to highlight here. That's not the way you framed it.

REP. HOLT: Well, what I was asking was, who makes the decision? And who oversees that decision? Who provides --

MR. McCONNELL: The same --

REP. HOLT: Who provides protection against the kind of thing that we see in oppressive governments around the world, a knock on the door in the middle of the night, somebody barges in and searches the place? Now we're just talking about figuratively, an electronic search, maybe not a physical search, although maybe we're also talking about that in this legislation.

The question is, who provides the kind of check and balance that Americans expect that will protect them against having their lives ruined by an overzealous government who is trying to protect the safety and security of the people or of the government --

MR. McCONNELL: There are three levels of protection.

REP. HOLT: -- or protect them from a government that would have an enemies' list, which you might say never happened here, but it has?

MR. McCONNELL: Three levels of protection.

REP. HOLT: So the question is, who provides what standard? And you just said, I thought, that operationally the person who does make the decision that it's okay to tap this phone or to intercept that communication would not make a decision any differently if the court were not looking over his shoulder, if they were not required to have a warrant, either now or maybe 72 hours later.

MR. McCONNELL: Three levels of protection. First of all, the initial judgment will be made the same way it's been made for almost 30 years. That's the professional that's doing the mission. It would be then reviewed internal to that organization. It would be reviewed by the Department of Justice. And, as passed in the law last month, the procedures for doing that would be reviewed by the court. The last level of oversight is this body, this committee. You can walk any time out to NSA and look at anything you want to see.

REP. HOLT: But you just said you can't give us that information. You said to Ms. Schakowsky, you know, you don't even really know who we've intercepted and whether they're Americans.

MR. McCONNELL: I said it might not be knowable. We can look at it and see if it's a knowable answer.

REP. HOLT: But that's not much reassurance to us that then we have to exert that oversight that nobody else along the way is exerting except a well-meaning political appointee, or maybe not-so- well-meaning political appointee, or a well-meaning but perhaps mistaken bureaucrat.

You know, these people are trying to do their jobs. They're trying to protect us. But we have to give them the guidance. Now, one of the things that concerns us is that, you know, the intelligence community, you, are particularly, more than anyone else in the United States, supposed to speak truth to power. And that means you have to keep a certain distance from that power to whom you have to speak the truth.

And that's why it concerns me that when you talked about the lawyers who were working to prepare this legislation back in August, when you made some of the statements that you made, they clearly seemed to be influenced by lawyers in power, in the White House, in the vice president's office. And that's troubling, actually.

You, of course, are a presidential appointee. But it is critically important that you keep a professional distance. That's why I asked these questions earlier today that I'm afraid you might have thought were insulting. But your credibility as an independent person is so important to our safety and security, so important to our rights as humans.

So, I mean, can you say that during those hours when this legislation was being written that your team of lawyers was not consulting with, say, Mr. Addington and his team of lawyers?

MR. McCONNELL: I would say was not influenced by a political process. I spoke truth to power. There's a team of lawyers that worked this, starting last year, and the team worked it throughout the past year and up to and including the period of time that we had the bill passed in August.

REP. HOLT: And how much consultation was there between your lawyers and the vice president's lawyers?

MR. McCONNELL: Extensive. And with the vice president's lawyers -- there was extensive consultation between the lawyers working the problem. I don't know who was working the problem in the vice president's office.

REP. HOLT: You know, forgive me if it seems insulting, but you have to take a step back about what it means to be able to speak truth to power and to have an independence in what we say that's permissible to do with Americans' lives.

MR. McCONNELL: I did.

REP. REYES:  Thank you, Mr. Holt.

Mr. Tiahrt, first round.

REP. TODD TIAHRT (R-KS):  Thank you, Mr. Chairman.

Last -- or this year, in a bipartisan fashion, we passed the Protect America Act.  It passed the House, passed the Senate, signed into law by the president.  Now, would you -- what would the impact on intelligence collection be if the Protect America Act were not renewed?

MR. McCONNELL:  We'd lost half to two-thirds of our capability specifically targeting terrorist groups because of the -- not the court, but the language of the law that the court had to interpret. And within a few days after passing the act, we were back up in full coverage.

REP. TIAHRT:  So the Protect America Act has helped enhance the speed and agility of the intelligence community?  Is that what you're saying?

MR. McCONNELL:  Significantly so, yes, sir.

REP. TIAHRT:  Okay, that's good news.  Now, we heard privacy advocates, outside and inside the committee, that have argued that the minimization processes are inadequate to protect Americans' privacy interest.  They take issue with the fact that the government may still capture and screen incidental communications, as we just heard, and even if no use is ultimately made of the contents of that communications.

Do you feel that the procedures adequately limit the government's intrusion into the protected communications of America?

MR. McCONNELL:  Sir, I do, because intrusion would be a violation of the law.  So the minimization procedures have been in effect for almost 30 years.  They work, and work well.  I had the pleasure and the privilege of serving as the director of NSA, and so there's a whole training-oversight-recertification program about how you would do that.  And so it's worked well. It's been subjected to the court and reviewed by the court and endorsed by the court.  So it's worked for almost 30 years.  REP. TIAHRT:  Well, is there a practical alternative to what you're doing now?

MR. McCONNELL:  No, sir, there isn't.  And that's one of the reasons that we've failed to communicate on a lot of these issues. Often someone would say, "Well, it's okay to foreign to foreign."  And what I keep attempting to highlight is you can only target one end of a conversation.  You can't control who that person at the other end might call.

More often than not, overwhelming majority -- I don't know the number, but almost always it would be a foreign-to-foreign communication.  But you can't guarantee it.  So if you make it a condition in the law that you have to guarantee ahead of time, it effectively shuts down your operation.

So in the condition that a foreigner called in and there's incidental collection, then it would be minimized.  If it's nothing of harm to the nation, it would be minimized.  If it was a potential harm to the nation, that might be our most important call.  Then we would take appropriate action.

REP. TIAHRT: If a terrorist is being monitored internationally, outside the United States, and someone from the United States calls in to that terrorist's phone number, and there is, in the mind of the agent, a probable cause to investigate that contact, for that citizen inside America that's made the phone call, is that held by your agency, or do you turn that over to the FBI to develop probable cause and complete the investigation?

MR. McCONNELL: The way you've described it, the target for my community would be the foreign person, foreign country. Once that call is made, as it was in the 9/11 situation -- it would subsequently be reported on by 9/11 and a joint commission of Congress -- that call was made, then the intelligence community would realize a U.S. person calling a terrorist.

It depends on the content of the conversation. If it turns out it's a terrorist operation, planning, whatever, refer to the FBI. The FBI would get a warrant against the U.S. person, the person located in the United States, and then do their normal surveillance mission.

REP. TIAHRT: So they would carry out the requirements of the Fourth Amendment of the Constitution as far as probable cause and the warrants and all those.

MR. McCONNELL: Yes, sir, under a warrant subjected to court review, or provided by the court.

REP. TIAHRT: The committee received testimony earlier this week that the FISA court should have to make probable-cause findings to protect every person who might potentially communicate with the target, and not just the target itself -- in other words, an incidental contact -- that probable cause would have to be achieved. What's your reaction to that proposal?

MR. McCONNELL: Effectively, sir, it shuts down our operation, because it creates a condition we couldn't satisfy in the eyes of the law. So that's why we're arguing for exclusion of where's the target, and is the target overseas? And as I've mentioned earlier, what we were caught in the old wording in the old law is because of where you intercepted it in this country is what caused the problem.

If it had been intercept in the foreign country and a different mode -- wireless -- it wouldn't have been a question.

REP. TIAHRT: So a majority of the contacts of communications of the target -- let me put it this way. Do foreign target communications mainly deal with foreigners and their contacts --

MR. McCONNELL: Almost always.

REP. TIAHRT: Almost always. Very seldom that it isn't.

MR. McCONNELL: I would -- it's a very tiny, tiny fraction of a percent.

REP. TIAHRT: Okay, but when that does occur, then -- and there is probable cause that's then turned over the -- another agency -- the FBI, to carry out --

MR. McCONNELL: You need a warrant, and if it were incidental -- meaning they called a pizza shop -- is of no intelligence value -- then you would take it out of the database.

REP. TIAHRT: I see.

So -- Mr. Wainstein?

MR. WAINSTEIN: If I could just add to that very briefly. And -- the argument that you've heard occasionally is that when somebody we're surveilling appropriately under this statute calls someone in the United States, that should then trigger a requirement for the government to get some kind of core process against the person in the United States. While that sort of has some gut-level appeal, I think, when you first look at it, you've got to recognize that that it is not a requirement in any of the regimes. For instance, on the criminal side -- Title III warrants. You get a Title III warrant against one person, that has a court authority -- it gives you court authority to surveil that person. That person talks to somebody else -- another American -- we don't have to go back to the court to get approval to listen to that person's communications.

So that's the way it is on the criminal side and on the foreign intelligence side. And as the director said, that's the only workable way of dealing with it. We just deal with it with minimization instead. MR. McCONNELL: If you make that other person your target now and you're going to listen to him intentionally, that becomes a subject of warrant.

REP. TIAHRT: Thank you.

For the record, I'd like to say that I think it's important that your lawyers communicate with those in the -- other parts of the administration and that we should not limit free speech whenever developing policy or looking at how we apply current law. So to limit contacts and free speech in order to make us move forward in this process, I would -- I would be opposed to that -- limits on free speech. I think that you should be in contact with other areas of the government and we shouldn't restrict it.

Thank you for your testimony.

Thank you, Mr. Chairman.

REP. REYES: Thank you, Mr. Tiahrt.

Mr. Tierney.

REP. TIERNEY: Thank you.

Director, I'm glad you made that last caveat because in fact, it -- if we have significant interception on a U.S. citizen or person in the United States, then of course you would need a warrant. And I think we all should understand that.

MR. McCONNELL: If there's a target, yes, sir.

REP. TIERNEY: You essentially get to the point where he's the target.

MR. McCONNELL: If he's a target --

REP. TIERNEY: It's determining when that crossover point is, I think, that has concerned some of us.

You also at one point earlier in your testimony said that there are perhaps billions of data or records --

MR. McCONNELL: Transactions.

REP. TIERNEY: -- transactions being done. So when you start with a small percentage, it's a small percentage of those billions that might sort of scoop in some --

MR. McCONNELL: Well, it's not -- what I was talking -- there are billions of transactions. We would have some subset of that. And when you work it down, it turns out to be a pretty small number. REP. TIERNEY: So a small percentage of billions in the subset and that -- it could still be a substantial number. I think that's the problem.

Now earlier this week, we got a letter from -- I think -- we, being the committee, got a letter from Mr. Alex Joel. I understand he's your civil liberties protection officer in your office, is that right?

MR. McCONNELL: That's correct, and I think he's with us here. He's sitting here this morning.

REP. TIERNEY: Joel, thank you.

Joel's letter says that -- it lays out the civil liberty and privacy protections that he believes his office is charged with overseeing in the implementation of the new act. Now I indicated earlier that one of my problems is that I don't think it ought to be the DNI's office overseeing the DNI. But set that aside for a second. Mr. Joel's letter states, among other things, that although he doesn't read the PAA to require it, the NSA is still using the minimization procedures that were previously reviewed and approved by the FISA court. Does that strike you as accurate?

MR. McCONNELL: Well, let's ask Mr. Joel. He wrote the letter.

REP. TIERNEY: He works for you, so I'm asking you. Or you didn't know this?

MR. McCONNELL: Oh, well, I'm -- well, restate the question. I thought you were asking him a question.

REP. TIERNEY: The question is that he says that the NSA is using minimization procedures previously reviewed and approved by the FISA court. Even though he doesn't read the PAA as requiring it, that's what's being done.

MR. McCONNELL: That is -- that's my understanding of what's being done currently, yes. And the reason for that, sir, is the court set the standard and it's been tested in court. It's a reasonable standard and it's good for us to follow it.

REP. TIERNEY: And did that in any way impede the process of implementing any of the new authorities under the PAA?

MR. McCONNELL: No to my knowledge.

REP. TIERNEY: All right.

Do you have an objection to requiring the FISA court to review the minimization procedures in any future FISA legislation? MR. McCONNELL: Sir. I'd be happy to take any recommendation suggestion you've got. And remember, I've tried to highlight several times -- very complex, and you want to keep asking me hypotheticals. You know, let's write it down, have my team look at it --

REP. TIERNEY: But my point --

MR. McCONNELL: Negotiate, and I can --

REP. TIERNEY: My point is that --

MR. McCONNELL: -- I'd be happy to look at anything you suggest, sir.

REP. TIERNEY: Well, this is something your office suggested because they're the ones that are doing it, all right? Mr. Joel has made the suggestion and is carrying out the fact that he's following those previous FISA procedures. And you said that that didn't in any way impede the operation under the new PAA, so I assume that you have no objection to that being written into the law -- that that's what we'll do at this point.

MR. McCONNELL: I have no objection to any recommendation you want to make. We'll be happy to examine it.

REP. TIERNEY: Are you opposed, then, to the FISA court having authority written into the law to do exactly what Mr. Joel is now doing on his own?

MR. McCONNELL: I'd be happy to take the language and examine it, sir. The point I keep trying to highlight --

REP. TIERNEY: Let me back up --

MR. McCONNELL: Is very complex --

REP. TIERNEY: Do you have an objection to Mr. Joel doing what he's doing now?

MR. McCONNELL: I have no objection to Mr. -- what Mr. Joel's doing --

REP. TIERNEY: All right. Fine.

MR. McCONNELL: -- what he's doing.

REP. TIERNEY: Let's go back to --

MR. McCONNELL: But what I'm trying to make sure everybody understands is we can't get ourselves in the situation we were before where we're forced under a time constraint -- you had a time constraint, I did not, and we were asked to -- REP. TIERNEY: We have our opinion on how that time constraint came to be, all right? And I want --

MR. McCONNELL: Sir, it was your schedule. Not mine.

REP. TIERNEY: No, it wasn't anybody's schedule. It was a political schedule, if you really want to get down to it.

MR. McCONNELL: Well, sir, that's a point of view.

REP. TIERNEY: That's a very strong point of view, and I think everybody realizes it now, all right? But the fact of the matter is that -- you know, we're trying to find a way to get to a law that everybody can --

MR. McCONNELL: We'd be happy to look at anything you propose.

REP. TIERNEY: I'm happy to know that Mr. Joel at least -- and apparently with your approval now -- sees no objection to the court looking at those procedures for minimization and approving them. His letter also notes that the NSA inspector general is conducting an audit of the implementation of the new act, and that the inspector general regularly conducts audits, inspections and reviews of compliance and minimization procedures. Why was that decision made that the NSA IG would conduct an audit on the implementation of the new act? Do you know?

MR. McCONNELL: It's been part of the process since the beginning, to my knowledge.

REP. TIERNEY: Okay. So I can assume, then, you would not object to requiring in the statute that the inspector general make those reviews and make those audits in the future with respect to any civil liberty protections -- to put into law what it is you're already doing.

MR. McCONNELL: Sir, I have no objection to anything you want to recommend. If we agree with the language --

REP. TIERNEY: I'm not talking about recommendations. I'm talking about do you have an objection to writing into law --

MR. McCONNELL: We'd be happy to consider --

REP. TIERNEY: -- the function -- what Mr. Joel says is now happening, the inspector general doing audits.

MR. McCONNELL: I'd say again, you -- let's write it down and let's examine --

REP. TIERNEY: I'm not writing it down. I'm saying -- it's not hard to understand. MR. McCONNELL: And then we'll agree to it.

REP. TIERNEY: Do you have an objection to the inspector general conducting audits, or do you not have an objection?

MR. McCONNELL: I do not have an objection to the inspector general conducting audits in NSA. They have when I was there. They still are. I have no objection to that.

REP. TIERNEY: Fine. That was very easy to get to. We didn't have to write it down.

Now earlier you talked about there being a large database, so making it improbable or difficult -- sometimes also impossible to determine the number of times that United States persons' communications that were inadvertently intercepted when you were going after a target in a foreign country --

MR. McCONNELL: That's not exactly what I said.

REP. TIERNEY: All right. Well, will you tell me again what you said?

MR. McCONNELL: Yes. I said we have no control over what foreign targets would talk about. And remember, it's to, from or about.

REP. TIERNEY: Mm-hmm.

MR. McCONNELL: So if a foreigner's talking about you and it's in the database, I may not know. I may -- could find it if I had a reason to go search for it.

REP. TIERNEY: Okay.

MR. McCONNELL: The database would age off in a period of time with the -- no harm, no foul.

REP. TIERNEY: But when somebody asks you for the number of times when U.S. persons or a person in the United States were involved in that situation, I think said that there was some degree of difficulty in getting that done.

MR. McCONNELL: I just don't know how difficult, but we'll look at it and see if we can answer the question.

REP. TIERNEY: Would it be reasonable to have a sampling done?

(Cross talk.)

MR. McCONNELL: We'll look and see. If we can give you the total complete answer, we will. We just -- I just don't know that we can, but we'll take the question and see what's doable.

REP. TIERNEY: Thank you very much.

Thank you, Mr. Chairman.

REP. REYES: Thank you, Mr. Tierney.

Mr. Ruppersrberger.

REP. RUPPERSBERGER: Yes. We've had two hearings two hearings with both of you. I know the hearings sometimes have been difficult -- a very sensitive issue -- and I'd just like to review where I think we are. To begin with, I think it's clear that we all agree that wire-tapping foreigners to obtain critical information to protect our country is allowed under the Constitution. I think we all agree to that.

Do we agree to that?

MR. McCONNELL: Foreign -- say it again, sir. Foreign -- in foreign countries --

REP. RUPPERSBERGER: Wire-tapping foreigners to obtain critical information in the war against terror, okay.

Now --

MR. McCONNELL: What we can't allow though, is when the wording in the bill would cause that to be in question or could be interpreted a different way.

REP. RUPPERSBERGER: Well, that's what we're looking for is clarity and we agree to clarity. And the one area I would get into, though, is, you know -- I've heard this and I want to clarify this, too. Why are you opposed to having court-review procedures -- this is procedures, not the individual cases -- after surveillance has begun? That's a concern of mine -- not when there's an emergency situation. You're not --

MR. McCONNELL: That's what we agreed to. That's in the law.

REP. RUPPERSBERGER: Well then, you know, I think we're getting very close here. And, you know, these hearings -- sometimes you wonder what you've accomplished. But I think after these hearings we should be able to come together and resolve this issue.

I think the biggest area that we have is that we must have judicial oversight. Our country is a system -- we have a system of laws. And when in fact the checks and balances go the other way we have problems -- no matter who's president. And I think what we object to is that there is not the independent judicial review. But we also understand the war against terror is a different war than we've had years ago and that's why we're attempting to resolve this.

I think we've agreed on most of the issues other than the judicial oversight. Now, let me ask you this also, this question: The minimization issue. When in fact you have an American -- where do you think the problem is that you see between certain members' point of view here and your point of view on minimization -- Mr. Wainstein?

MR. WAINSTEIN: I'm not sure exactly which members you're referring to, but I think some have voiced some concern that minimization isn't sufficient, that we need to get some kind of court approval before we listen in on communications appropriately intercepted against a person overseas, but that are sent into somebody in the United States.

REP. RUPPERSBERGER: I would think -- what I understand from what I'm hearing, and what my concern would be on the issue of minimization, is that when a court's -- what a court does as far as the oversight, that minimization takes the place of that. I think that's something that we could work out.

MR. McCONNELL: Well, sir, in fact, the issue becomes --

REP. RUPPERSBERGER: Yeah, sure.

MR. McCONNELL: What frequently people slip into is everybody's in agreement a foreign-to-foreign communication shouldn't be an issue, but if you make that a precondition -- what we keep attempting to highly is you can't determine that ahead of time. So if you make it a precondition in the law you've effectively shut us down from doing --

REP. RUPPERSBERGER: From what I understand and what we're talking about today and you said, what would happen if the FISA bill didn't go forward. And I think we need to clarify that too. We're not talking about not having a bill. We are so close on what we have negotiated and you know that and I know that. There's --

MR. McCONNELL: Sir, all I'm arguing for is keeping the minimization --

REP. RUPPERSBERGER: So I think to say that if we didn't have a FISA bill that we would be put at risk -- we're not talking about that, neither side is. What we're talking about and the one issue is that we need to have a judicial review. But we understand there are emergency situations when an American's at risk -- when somebody's contacted. And that has to do, I think, more with operations and giving people the resources. If we need to hire more judges, if we need to hire more people in CIA and NSA to do this, we'll what we have to do.

MR. McCONNELL: And we now have judicial review -- that process that Mr. Holt was making reference to about our dialogue and who we talk to. That's how the judicial review was proposed, agreed to and put in the bill. We have that judicial review.

REP. RUPPERSBERGER: What the law basically says today -- the law that was passed that we have to look at -- is that basically, under the circumstances -- I don't think that you want this or we want this -- is that our government has a right to basically have the search and seizure of an American without a court order and without the Constitution being involved. We fight for liberties and freedom and part of that is what --

MR. McCONNELL: Sir, I agree with you 100 percent.

REP. RUPPERSBERGER: So bottom line, you know, I think that we -- if you agree with that, then I'm not sure where our arguments are. But we're only asking for the court to come in and review the process --

MR. McCONNELL: And that's where we --

REP. RUPPERSBERGER: -- not individual cases. That's not what it says. This law basically says that our government can have a search and seizure of American citizens and that's where --

MR. McCONNELL: No, sir. It doesn't say that at all.

REP. RUPPERSBERGER: -- oh, I disagree with that interpretation. But if it does, then we don't have clarity and we if don't have clarity we have to fix it and that's our job as members of Congress.

Yes?

MR. WAINSTEIN: If I may just briefly respond to that: Just keep in mind, as the director said, when we target surveillance on a person -- a person overseas -- we target against that person. If that person calls into the United States, we subject any of the information we get about the U.S. person to minimization. That's actually the only practical option. And in fact, that's what we do on the criminal side too.

As a prosecutor I get a court authorization to do a Title III wiretap against Defendant A -- he might talk to 1,000 people. We don't go get court process for everyone of those 1,000 people. So as long as we have it against the target, we're allowed to collect and minimize that person's communications with everybody else. That's the only way this works, because otherwise --

REP. RUPPERSBERGER: That's not what it works -- you're talking about what the law says and what you can do. And it's not about who you are, you are -- we're gone. Somebody else comes in. We need to clarify it. When the president comes to the district I represent and says that we need to go further than we are now when we know -- when I feel that we will be able to give you what you need to protect our country, that's where we are. But our Constitution is what we fight for -- in Iraq, in World War II, the Korean War, the Vietnam War -- and we have to keep focused in that. That's our jobs. Those are our jobs.

MR. WAINSTEIN: Agreed.

REP. RUPPERSBERGER: Thank you.

REP. REYES: Thank you, Mr. Ruppersberger.

The director and Mr. Wainstein, I'm told, have another hearing on the Senate side. So Mr. Tiahrt will be the last person to have an opportunity to ask questions for five minutes.

Mr. Tiahrt.

REP. TIAHRT: Thank you. And God forbid we should hold up the Senate. (Laughter.)

MR. McCONNELL: Go ahead, sir. It's going to be an interesting hearing over there too.

REP. TIAHRT: I'm sure it will be.

I read the law before we voted on it and I fail to see anywhere where we allowed search and seizure of American information or any of their communications without having some kind of a -- without having the methods that you use currently.

MR. McCONNELL: Yes, sir.

REP. TIAHRT: The Protect America Act provided for the update from the 1970s law FISA to allow us to move into the electronic age, basically.

MR. McCONNELL: That's correct.

REP. TIAHRT: So now I think we're taking -- it sounds to me, from what we've had in our discussions this morning that we're taking scenarios that may or may not exist and hoping to write some laws to involve more lawyers and judges in the process. And so far I haven't found any evidence or heard of any instances where you have violated the constitutional rights of American citizens. So I guess maybe we're extending beyond that and that we're looking at foreign citizens having the same constitutional rights that Americans have. And I think most Americans would say that those who intend to destroy this country should not have the same rights that we have fought for and paid for in blood and that's embodied in our Constitution.

So is there -- if you follow your procedures and we're satisfied with your procedures, would you see a need for Congress to write a law for every procedure that you have that you're currently following? Is there a need for that that you see?

MR. McCONNELL: No, sir. In my opinion, no. And my worry is what might be captured could have an unintended consequence. Right now the negotiation we had in July and early August, the court now does review all those procedures. So I'm satisfied that based on our lessons learned from '78 to the current time frame, tried and tested our minimization process and so on, I'm satisfied that it works to protect American civil liberties and it allows us to do our mission of overseas intelligence against foreigners. And my worry -- the reason I hesitate to agree to any specific point is it could cause us to not be flexible and capable in our overseas mission if we don't say it just right. And what is in the law today works well and I'm very hesitant to agree to any changes to that.

REP. TIAHRT: So we're abiding by the Constitution --

MR. McCONNELL: Yes, sir. REP. TIAHRT: -- with our updated law -- Protect America Act --

MR. McCONNELL: Yes, sir.

REP. TIAHRT? -- and we have judicial overview of minimization and of contacts with Americans, if they are contacted in the process of accumulating data.

MR. McCONNELL: And we have reports to this body every six months. And as you need to you're welcome to look at any aspect or any part of it.

REP. TIAHRT: Is it fair to say that today's proceedings are congressional oversight, or do you think we are avoiding our responsibility of congressional oversight?

MR. McCONNELL: No, sir. I don't think your avoiding your responsibility. I'd just like to get more of the members to sit down and look at the data and understand it and have a feel for it, have an opportunity to meet the people that actually do this and their professionalism, their commitment to also protecting civil liberties. They're very, very serious about it. So it gives you an opportunity to get some confidence in the process.

REP. TIAHRT: Well, I'd like you to pass along to all those who you're responsible for working here in the government for -- thank you for the last six years of safety: No attack on our homeland, and I know there have been many, many attempts.

And I'm glad that we were able to update the law to move ourselves as a country into the electronic age, instead of trying to proceed under the old law that was written. And I too am very hesitant to inject more lawyers and judicial process into the system, which appears to only slow things down and makes us in essence less safe. I mean we, because of leaks, have not been able to collect phone data as we have in the past -- before the Protect America Act. Now I think we've improved that significantly. We haven't been able to contact and follow e-mails as we did, because of leaks in the past. We haven't been able to follow financial transactions because our allies do not cooperate -- back to leaks that occurred here in this country. All of those leaks, I believe, were intended to embarrass this presidency and all of them have made it more difficult to do your job to keep this country safe. So in spite of all of that difficulty and overcoming all those obstacles, I want to thank you and the people that work for you for keeping this country safe for the last six years.

I yield back.

REP. REYES: Thank you, Mr. Tiahrt.

And let me add my thanks for the work that you, Director McConnell and Mr. Wainstein, do for our great country. And as was evident today in our hearing, there are a variety of opinions, different concerns. One thing that we want to do is work together to give the tools necessary to those that are in charge of keeping us safe.

So gentlemen, thank you for being here. We appreciate your service to our nation.

And the hearing is adjourned. (Sounds gavel.)

END.

Exhibit 18

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; AMERICAN CIVIL LIBERTIES UNION OF MICHIGAN; COUNCIL ON AMERICAN-ISLAMIC RELATIONS; COUNCIL ON AMERICAN-ISLAMIC RELATIONS MICHIGAN; GREENPEACE, INC.; NATIONAL ASSOC. OF CRIMINAL DEFENSE LAWYERS; JAMES BAMFORD; LARRY DIAMOND; CHRISTOPHER HITCHENS; TARA MCKELVEY; and BARNETT R. RUBIN,
Plaintiffs,

v.

CIVIL ACTION
NO. 06-10204

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; and LIEUTENANT GENERAL KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service,
Defendants.
_______________________________________/

MOTION FOR PARTIAL SUMMARY JUDGMENT
BEFORE THE HONORABLE ANNA DIGGS TAYLOR
United States District Judge
231 Lafayette Boulevard West
Detroit, Michigan
Monday, June 12, 2006

APPEARANCES:

American Civil Liberties Union Foundation
MS. ANN BEESON
125 Broad Street-18th Floor
New York, New York 10004
(212) 549-2601
On behalf of Plaintiffs.

United States Department of Justice
ANTHONY J. COPPOLINO
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
(202) 514-4782
On behalf of Defendants.

- - -

**TO OBTAIN CERTIFIED TRANSCRIPT:**
Andrea E. Wabeke, CSR, RMR, CRR
734.741.2106 x1144

where they put in declarations and testimony that they were no longer willing to use certain lands that they believed were polluted.

So like this case, the harm was a result in part of the plaintiffs' own behavior in response to the government action -- in response to the action being challenged. In that case, the plaintiffs were harmed because the alleged polluting of the land was preventing them from enjoying the land. Here, of course, it's the warrantless wiretapping by the NSA that has led directly to the Plaintiffs' decision to cease certain confidential communications with clients and sources.

Do you have any additional questions about the standing, your Honor?

THE COURT: That's all. Thank you.

MS. BEESON: Thank you very much.

THE COURT: I think we can go ahead to the next.

MR. COPPOLINO: Good morning, your Honor. Your Honor, I'm Anthony Coppolino. I'm an attorney with the Department of Justice civil division in Washington representing the United States in this case.

Your Honor, I'd like to just start by

observing that the injunction that the Plaintiffs seek in this case is among the most significant they could ever ask the Court to consider. Plaintiffs ask the Court today to enjoin a program that the President of the United States has determined is necessary to detect and prevent another foreign terrorist attack on the United States by the Al Qaeda terrorist network, a network that as we all know has already killed thousands on American soil.

They seek this injunction on the grounds that the surveillance program that the President has authorized intercepts one end foreign calls, that is, calls going to or from the United States, and that it allegedly exceeds the President's statutory and constitutional powers for the reasons that Miss Beeson has just outlined.

Now, your Honor, contrary to Plaintiffs' assertion, the Government is quite confident the President's actions are directly and narrowly focused on the Al Qaeda terrorist threat and are well within his lawful authority. The President has explained the extremely serious nature of that threat. It has been four years since 9/11, but the threat has not diminished. In addition, the President has explained that he authorized the program that is targeted specifically at Al Qaeda related communications, communications that involve agents or members of Al Qaeda and affiliated terrorist organizations.

Your Honor, the dilemma the Government faces, however, in responding to the Plaintiff's' motion for summary judgment is that the evidence needed to demonstrate to you the lawfulness of the President's surveillance program, which we call a terrorist surveillance program, the evidence necessary to demonstrate to you that it is lawful cannot be disclosed without that process itself causing great harm to the U.S. national security.

That is information that would explain the threat that the President has acted to address, the actions that he specifically authorized and who is subject to surveillance and why. And that is information that is subject to the state secrets privilege assertion that we have lodged in this case by the director of national intelligence, supported by a declaration from the National Security Agency.

Your Honor, it's as a result of this claim of privilege that critical evidence is not available in this case. Plaintiffs argue nevertheless that the case can proceed based on a scant public record, and that's what their motion for summary judgment is based on. We think that it is clearly wrong. This case does not involve easy questions, as Miss Beeson just said.

It is not a simple case. It is a case which requires a robust factual record. Whenever a court is asked to enjoin the President's powers, particularly in the area as commander in chief seeking to detect a foreign enemy that seeks to attack America on its home land, it could not possibly decide it and argue without conceding the full -- considering the full scope and contours of what the President's done.

The key issue in the case, as Miss Beeson identified, is whether the President's actions fall within congressional authority and if not, where the line is drawn between the President's own power to detect and prevent a terrorist attack, and Congress' ability to regulate the President's actions. And that issue critically depends on the facts.

Without evidence that goes to the heart of the matter, the Plaintiffs' claims cannot be addressed. And specifically, your Honor, to demonstrate that the Plaintiffs' claims are meritless would require explaining to the Court what specifically the President authorized, specifically why he authorized them, specifically how those activities are undertaken. Those facts --

THE COURT: Well, excuse me, you have conceded, have you not, that a program has been authorized?

MR. COPPOLINO: No question. In December 2004, the President acknowledged the existence of the program. There are many more facts, as we set forth in our in camera submissions to you, which would demonstrate that the facts regarding how that program is operated, the specific nature of the threat that it seeks to detect and prevent, are facts that are relevant to judging whether the President's actions are lawful. They're also very relevant to judging the merits of the Fourth Amendment claim and the First Amendment claims, which are inherently factual.

There was a recent case, your Honor, in the Fourth Circuit -- actually, well this case called **El Masri** in the Fourth Circuit, in which the court seized on the very distinction that you just made, and that is there's very much a difference between the existence of an activity and the details of that activity. That was a case that involved an alleged CIA rendition program, an individual who claimed that he had been rendered to another foreign country and treated very badly and sued in federal court here in the United States, and the court dismissed the case on state secrets grounds. We've cited this in our papers to you.

And the court said: I know that there may be acknowledgment of the existence of a program, but there are very critical state secrets about how that program runs, and those secrets are important to understanding whether it's -- whether the program is lawful and how it proceeds.

And our first response to you today, your Honor, with respect to summary judgment is that the full breadth of those facts are necessary for you to understand exactly what's going on here, and for you to make a determination as to whether the President's actions were lawful. Beyond that, perhaps even more fundamentally as a threshold matter, those facts are essential to determining some very basic threshold issues.

One is Plaintiffs' standing. I'd like to address that issue a little bit further. But secondly, aside from the issue of standing -- let me just say on the issue of standing, the facts are critical to determining whether or not the Plaintiffs in fact have standing. Even if you think they've alleged sufficient injury, and we don't and I'll explain why, but even if you thought they did allege sufficient injury, that doesn't end the standing issue.

As you well know, standing can be considered further on summary judgment and is an issue of fact. We don't believe the facts that are necessary for the Plaintiffs to establish standing are available, primarily because for the very simple reason the Government is not in a position to confirm or deny who may be targeted and who may not be, because that itself is revealing of highly significant, sensitive, classified information.

And furthermore, we're not in a position to disclose the specific contours of how our program operates in order to address these allegations that it somehow covers these Plaintiffs. So the facts are critical to Plaintiffs' standing. In addition, your Honor, perhaps more importantly, it depends on your point of view, the facts are critical to the Government's defense of the case. And in our classified submission, we've set that forth for you in great detail.

Now, we've asserted the state secrets privilege because we are confident that the information that the information that is necessary to litigate this case cannot be disclosed. We've not asserted this privilege, contrary to any suggestion you might hear from Plaintiffs or in the media, to cover up allegations of wrongdoing. You will see in our materials exactly why we have submitted this -- exactly why we have asserted privilege as to this information.

We explained to you in our classified submission the information at stake, its relation to the merits and the harm of disclosure. And so with that as sort of back drop, your Honor, I'd like to just address some of the points that Miss Beeson addressed, which are the consequences that flow from the state secrets claim.

By way of background, the state secrets privilege has been around for many years and I've detailed this in my brief, so I'm not going to go into this a great deal. It's not an ordinary privilege. It's one of the highest significance. In fact, every court that has considered it has so characterized it as a privilege that heads the list of Government privileges. It's been asserted in this case, your Honor, because the case on its face puts at issue a classified national security intelligence activity.

There's no doubt about that.

And the details of that activity implicated by Plaintiffs' motion are set forth in our papers. But in brief, as I've already indicated, information that goes to the Al Qaeda threat, information about how the program operates, information that would tend to confirm or deny who's targeted are the key facts. And those are the key facts for them to make their case for us to defend and for the Court to decide.

In addition, there's state secrets privilege also makes clear that if the case itself concerns a classified activity, the very subject matter of the lawsuit is a classified activity. The case should not proceed because it will either require or risk the disclosure of classified facts as you attempt to adjudicate it.

Now, the standard for review in judging a state secrets privilege claim is highly deferential to the Government. That's set forth in all of the cases we cited. Judge Freeman's decision in the **Jabara** case many years ago for which this is a virtual replay in some respects -- in many respects sets forth that standard.

And he makes clear that the standard is whether there is a reasonable danger that disclosure of the information that's implicated by this case would harm U.S. national security. If that's shown, the information first must be protected. Judicial review on that question is not de novo, it is deferential to the Government's judgment as to why disclosure of information would harm national security.

The litigants' need for the information is not irrelevant to deciding a state secrets privilege claim. It is an absolute privilege. The only relevance of the need for the information -- that the need for the information has in the lawsuit is whether the Government has made a sufficient showing that it is in fact subject to the privilege and needs to be disclosed to protect national security. That's the only relevance of need. So if the information is essential, we have to make a showing to you that the information is in fact privileged and its disclosure would cause harm.

Now, obviously I'm not in a position to delineate the specific harms of disclosing that information. I'm not in a position to even describe the information any further. I'm confident, however, that when you do review our claim of privilege, you will agree that we've identified facts that are relevant. We've identified facts that cannot be disclosed. That's the first question. The information at issue in the privilege claim has to be excluded.

The second issue is what's the consequence of that? And that's really where our response meets Plaintiffs' motion for summary judgment. What is the consequence of our motion to dismiss based on the state secrets assertion on their motion for summary judgment? Well, your Honor, courts have identified three possible consequences of excluding information based on the states secrets privilege.

One is that the Plaintiffs could not make their case, and the second is that the Defendants cannot defend without the evidence, and the third, as I indicated, is that the lawsuit itself is so inherently involving state secrets that it could not proceed. Now, we think all three of these consequences apply here.

The Plaintiffs think they have enough facts as to obtain summary judgment. We don't think they have enough facts to obtain standing, but in any event, we're confident that we cannot present the defense that we need in order to defend the President's actions.

Let me talk first about the issue of standing, because that of course is a threshold issue. Perhaps the most central way in which a party can respond to summary judgment is the question of standing. Now, the Plaintiffs have made two allegations that would support their standing or two central arguments that would support their standing. And one is this issue of having to -- one is that they have been actually intercepted under the program, a claim of actual injury. And another is that they've had to modify their behavior as a result of the program. I'd like to address both of those.

And our response on standing, your Honor, is actually twofold, one of which has nothing to do at all with the state secrets privilege. And that is, first, we think that the allegations on the face of the complaint are insufficient to satisfy the requirements of standing. And second, if you did think those allegations were sufficient, they couldn't prove standing based on the facts. But let me talk about the first one.

Their allegations have been somewhat of a shifting target from their brief to brief, but they have argued first that their activities have been chilled as a result of the existence of a program, that they've had to modify the way in which they communicate. There are basically two categories of Plaintiffs and two categories of communications that I think you need to distinguish, although the end result of the legal analysis is the same.

One is some of the Plaintiffs are journalists and scholars who communicate with individuals overseas in the Middle East and Asia about current affairs, academic matters, political matters and so on. And they claim that as a result of the terrorist surveillance program, they are inhibited in their ability to do that. The second group of Plaintiffs, as Miss Beeson has pointed out, are attorneys who represent clients that have been accused of terrorist related offenses.

Now, I'm going to be talking about both of these types of allegations, but I want to make two points first. One is that it is not simply the case that they are chilled based on the way other people have been reacting to them. If you read the complaint, it is very clear, they are alleging that they are chilled as a result of the state -- as a result of the terrorist surveillance program. They also allege, primarily in their reply, that the reactions of other people who are chilled have caused them to modify their behavior. Neither allegation is sufficient.

Let me first talk about some of the allegations regarding general communications overseas. A number of the Plaintiffs allege -- these are generally the nonlawyer Plaintiffs -- that as a result of the terrorist surveillance program, they feel inhibited from talking about political topics, Islam, the war in Iraq and Iran, Israeli-Palestinian matters, human rights issues in China, things of that nature, journalists who want to talk with sources about Iraq, Afghanistan, a whole range of newsworthy topics, political topics, academic topics.

None of this has anything to do with this lawsuit, your Honor. The complaint on its face challenges a program which intercepts the communications of Al Qaeda. It does not -- it does not -- there's nothing to suggest that it somehow intercepts a wide swath of communications generally about political topics, research matters, human rights in Baluchistan or China. It is simply a non sequitur for a plaintiff to come in here and say that because the President is intercepting Al Qaeda, I cannot speak with someone overseas about human rights in China or about Islam generally or even the war in Iraq.

The whole basis of their allegations assumes that the program is targeted at subject areas. That's not what the President has said. The President has said it has targeted the interception of Al Qaeda communications. So on their face, to the extent they are arguing that they are chilled because they cannot speak with individuals overseas about a range of public interest topics, there's no standing at all. Those allegations are completely insufficient.

Now, in addition -- let me just address first of all those individuals who claim -- actually, let back up. I want to talk a little bit about **Laird** because you had asked specifically about that, **Laird** and some of those other cases. Now, the law is quite clear that allegations of a subjective chill in your communications as a result of the existence of a surveillance program is not enough to establish standing.

And by the way, your Honor, the point that they attempted to distinguish **Laird** on, that it dealt with an alleged lawful program, is something that is not a valid point of distinction. Courts have subsequently made clear that even if you alleged that the surveillance program is unlawful, and you've seen a couple of cases on that, the **Halcon** case, the **United**

**Presbyterian** case in the D.C. Circuit, even if you allege the program is unlawful, allegations that you are chilled by that program, that you have modified your behavior are not sufficient to establish standing.

And what the Supreme Court said in **Laird** is very important. For a chilling effect to be a cognizable injury, the challenged action must be regulatory, proscriptive or compulsory in nature. Standing has to be based on specific actions against them. It cannot be based on how they perceive the program and how they perceive the program might cover them. Not sufficient for standing.

The D.C. Circuit, relying on **Laird** in **Halcon versus Helms**, 690 F.2d 977 rejected standing in precisely the circumstance we face here. Actually, they did it twice. They did it in **Halcon versus Helms** and they did it in another case that then Judge Scalia decided as a circuit judge called **United Presbyterian Church versus Reagan.** In both cases, the plaintiffs allege that they were subject to surveillance under a program announced by the Government.

And in particular, in **Halcon** and in **United Presbyterian**, the plaintiff said that they engaged in certain activities which made it more likely that they would be targeted than most other people. In particular, they said they had numerous contacts with individuals overseas, just as these plaintiffs do.

And the court in both of those cases said that's not sufficient, and in **United Presbyterian**, the court said standing may be found based on an alleged chill only in situations in which the plaintiff has unquestionably suffered some concrete harm, past or immediately threatened, apart from the chill itself.

By the way, Judge Freeman made the very finding in the **Jabara** case many years ago. 476 Federal Supp 561. In **Jabara**, just by way of contrast, Jabara was found to have standing in a case involving alleged unlawful government surveillance because he in fact had been investigated by the Government for eight years. He'd been subject to FBI surveillance, NSA surveillance, physical surveillance, investigative reports about him had gone back and forth across the Government, and the court -- Judge Freeman said in that case he had standing, because the investigations clearly intruded into his life. There were facts to show that. It was actual injury. But you don't get standing simply by saying the President has a program and I'm concerned that it might cover me.

Now, Miss Beeson made a point that I think is clearly incorrect with respect -- she cites language in **Laird** which suggests that there is no standing if you're merely relying on a subjective chill without more. Those words, without more. She says if we allege more injury, we'd be **Laird** and we'd have standing, if we allege more than a subjective chill.

Well, first of all, your Honor, that just plainly misreads the case and it misreads other cases that they have cited. The without more phrase in **Laird** doesn't refer to what they allege. It doesn't refer to the plaintiffs alleging more injury. It clearly and obviously refers in those cases to something more that is done by the Government to them. That's the something more that the court in **Laird** and the cases applying **Laird** refer to. And so in other words, if a plaintiff is alleging more than not that they're merely chilled, but that the Government is doing something directly to them, then they might have standing.

A great example of that is the case I just cited in **Jabara**, where the plaintiff came in and said I'm not challenging the existence of a program and arguing that I'm chilled by it, they are investigating me and they're passing reports around about me. I'm injured. The court said you're injured.

Several of the cases that they've cited in support of their position prove just the opposite. In particular, there's a case called **Ozonoff versus Berzak** in the First Circuit cited in their papers. This was a case decided by then Judge Breyer, now Justice Breyer, 1984, and he specifically made that point, that the something more required of **Laird** is some additional action taken by the Government to the detriment of the plaintiffs. It is not whether the plaintiffs simply allege more injury. Any plaintiff can allege more injury. They said well, we're not just chilled, we're changing our behavior and therefore we've gone beyond **Laird**.

The other point to make I would hope is sort of an obvious point. The additional more that they are alleging is still no more than the consequences of the alleged chilling effect. Even in **Laird**, and in **Halcon** and in **United Presbyterian**, the plaintiffs weren't saying that we're just chilled. They're saying that our conduct is being effected. Our behavior is being effected by the existence of the program, just as these Plaintiffs are arguing here. So they didn't just say well, we're chilled.

What does chilled mean anyway? It means

that there's something that you're doing in reaction to the existence of a program to modify your behavior because you think you're being surveiled. That's what it means to be chilled, and that's all that these long declarations they've submitted have alleged. A terrorist surveillance program exists and as a result, we're doing something different.

But it fundamentally begs the question of standing. Did the Government do something to you directly under this program? And the answer is there's no allegation about that. And what's causing you to modify your behavior? Is there a regulation on you that's causing you to modify your behavior, or are you just doing it because you believe subjectively that you need to in order to avoid this program?

And so all of these additional injuries Miss Beeson has discussed, and all of them outlined in their declarations, are the same chilling injury. It's the same thing. It is the manifestation of the chill, if you will. And virtually all of the cases that they cite, your Honor, I could run through the list if you like. We do have another opportunity to file a brief in a few weeks. I could do it there too.

But virtually every single case on standing that they cite involves someone who is actually injured. Let me just give you one example. Case called **Clark versus Library of Congress**, which they cite. An individual who claimed that he was being investigated, and the issue there was well, did he have standing based on **Laird**. And the court said he did because there was an actual investigation of him.

Like Mr. Jabara, he was investigated, and furthermore, he claimed he was not promoted. He was challenging specific government action against him. He wasn't challenging a system of surveillance and saying that that system might cover me. He's saying you're doing something to me and that's what why he has standing there.

And that's the case in a number of other cases that they cite. Every single case they cite that I've read involves a plaintiff or plaintiffs that have an actual injury as a result of government conduct, and that's the key. If you cannot show that you are being regulated, that the Government has taken an action against you -- surveillance action or is about to, you haven't plead sufficiently to obtain standing.

Now, your Honor, I should add that I don't think that the allegation that other individuals are chilled adds anything to their standing argument. If the Plaintiffs couldn't establish standing on their own on the grounds that the existence of the program has caused them to modify their behavior as a result of being chilled, they couldn't possibly establish standing by arguing that it's chilled the activities of other people and therefore that has affected them.

In cases where courts have found that regulations of third parties have created standing for a plaintiff, the court has made very clear that the regulation of the third party causes an actual injury to the plaintiff, but there must be an actual regulation at issue.

For example, in the **United Presbyterian** -- not **United.** I think it's just called **Presbyterian Church versus United States**, which they cite in their brief, and it's very similar to the **Socialist Workers Party** case that Miss Beeson just talked about this morning. There, the third party being injured was an alleged group of people. In the **Socialist Workers Party** case, it was the Socialist Workers Party. The **Presbyterian Church** case, it was individuals that went to the **Presbyterian Church.**

Now, in **Presbyterian Church**, what happened was the Government went to the services and surveilled people. The Government actually showed up and started monitoring. And as a result of that actual action by the Government against those targets, the court said, well, there was a decrease in attendance at church and people were concerned but it was not speculation, it was something the Government did.

Here, their claims of standing are based on allegations that we're actually surveilling them and those are just based on an assumption that is not founded in fact. It sounds like, and I haven't read this case because she didn't cite it in her brief, it sounds like the **Socialist Workers Party** case is the same thing. The Government attended the meeting or threatened to attend the meeting, and therefore it was an actual injury to those who were there.

The point I'm trying to make, your Honor, is that if you want to get standing based on an allegation of subjective chill, the Government must actually do something to you and that must be clear. You don't have standing just by saying a program exists, we're modifying our behavior because we think it might cover us, and that's what their claims are, and it's not sufficient.

Now, let me address more specifically the argument that those attorneys who would represent terrorist clients have standing. I certainly recognize that in that respect, those plaintiffs come closer to being in the ballpark with the terrorist surveillance program, as opposed to the plaintiffs who say I'm inhibited from talking to my families in the Middle East and Asia, as if that somehow everybody in the Middle East and Asia is related to Al Qaeda, or I can't talk about political topics, or I can't talk about the war or I can't talk about human rights in China. Those folks are out of the box completely. Those attorneys who say, however, I represent Al Qaeda, they seem closer to being within the framework of the terrorist surveillance program.

But a couple points about that, your Honor. One is, as the court in **United Presbyterian** pointed out in the D.C. Circuit case, claims by a plaintiff that they're more likely for some reason to be subject to surveillance based on their activities is not enough. It may indeed be the case that plaintiffs who represent terrorist suspects are more likely to be subject to the program, but that doesn't adequately establish standing because it still doesn't show that they've actually been subject to any surveillance.

Judge Scalia wrote: That kind of allegation does not adequately aver that the specific action is threatened or even contemplated against them. And so even as to those plaintiffs, we would argue that they have not sufficiently alleged, that is those plaintiffs who allege they deal with terror suspects, we would argue they've not specifically alleged that they have standing.

Nonetheless, if you think that at least those Plaintiffs have sufficiently plead standing, I don't think it's possible that the Plaintiffs who merely speak overseas have, but if you think that those who claim they speak for terrorists have standing, and I don't think they have alleged enough, here's the key point in our standing argument, your Honor. The facts available for them to prove that and for us to defend it are not available. We've set this forth in our state secrets privilege.

Actually, this is the one point of our state secrets privilege that you could decide on the public record. In the public declarations of the director of national intelligence, Ambassador Negroponte, and the NSA, in the public declarations we have explained this particular point that goes to standing, which is that the Government cannot confirm or deny whether a particular individual is subject to surveillance or what the criteria is for subjecting individuals to surveillance.

# Exhibit 19

**DEPARTMENT OF THE TREASURY**
**WASHINGTON, D.C. 20220**

FAC No. SDG-392566
[redacted]

Date: February 6, 2008

**MEMORANDUM FOR** **ADAM J. SZUBIN**
**DIRECTOR**
**OFFICE OF FOREIGN ASSETS CONTROL**

**FROM:** Howard Mendelsohn HM 2/6/08
Deputy Assistant Secretary, Office of Intelligence and Analysis

**SUBJECT:** (U) Redesignation of Al-Haramain Islamic Foundation locations in the United States (**AHF-OREGON**), and AHF official **Soliman AL-BUTHE** pursuant to E.O. 13224

(U) INTRODUCTION

(U) President Bush issued Executive Order 13224 (E.O.) on September 23, 2001 declaring a national emergency to address grave acts of terrorism and threats of terrorism committed by foreign terrorists, including the September 11, 2001 terrorist attacks in New York, Pennsylvania, and the Pentagon. The E.O. authorizes the Secretary of the Treasury, in consultation with the Secretaries of State and Homeland Security,[1] and the Attorney General, to designate those persons determined to be:

(1) owned or controlled by, or to act for or on behalf of those persons listed in the Annex to the E.O., or those determined to be subject to subsection 1(b), 1(c), or 1(d)(i) of the E.O.;
(2) assisting in, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed in the Annex to E.O. 13224 or determined to be subject to the E.O.; or
(3) associated with those persons listed in the Annex, or those persons determined to be subject to subsection 1(b),1(c), or 1(d)(i) of the E.O.

(U) The following evidence in the files of the Office of Foreign Assets Control (OFAC) provides reason to believe that the entity and individual named below satisfy the criteria for designation pursuant to Executive Order 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."

(U) [Note: The name of the individual and entity proposed for redesignation in this memorandum will appear throughout the following text in **BOLD CAPITAL** font, while the names of persons previously designated as Specially Designated Global Terrorists (SDGT) pursuant to E.O. 13224 will appear in **Bold Title** font.]

[redacted]
Derived from: Multiple Sources
Declassify on: [redacted]

[1] (U) E.O. 13224 was amended by E.O. 13284 (January 23, 2003) adding the Secretary of Homeland Security to the consultative process.

For Case # 07-CV-1155-KI
U.S. District Court for the
District of Oregon 3/3/08

(U) ENTITY

(U) **AL-HARAMAIN ISLAMIC FOUNDATION** United States locations:

(U) 1257 Siskiyou Blvd.
Ashland, OR 97520

(U) 3800 Highway 99 S, Ashland, OR 97520-8718
[Source: Exhibit 88]

(U) 2151 E Division St.,
Springfield, MO 65803
[Source: Exhibit 87; United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95][2]

(U) INDIVIDUAL

(U) **Soliman AL-BUTHE**
(U) a.k.a. **Soliman AL-BATAHAI** a.k.a. **Soliman Al-BATHI** [redacted]
(U) DOB: 12/8/1961
(U) POB: Egypt
(U) Nationality: Saudi Arabia

2 ([redacted] Additional Al-Haramain Islamic Foundation locations are identified below.

([redacted]

(U//FOUO) P.O. Box 69606
Riyadh, Saudi Arabia 11557
[Source: www.arriyadh.com, accessed on 12/23/2003, Exhibit 52]

[redacted]

([redacted] [Source: AHF 2000 Annual Report in Arabic, Translation of pertinent parts, Exhibit 50; [redacted] www.arriyadh.com, accessed on 12/23/2003, Exhibit 52; [redacted]

(U) Saudi Arabia Passport #: B049614
(U) Saudi Arabia Passport #: C536660
[Source: www.un.org/sc/committees/1267/pdf/consolidatedlist.pdf, Exhibit 192]

(U) BACKGROUND ON AL-HARAMAIN ISLAMIC FOUNDATION

(U) OVERVIEW

(U) Ever since the terrorist attacks of September 11, 2001, a prime target of the United States' efforts to thwart the funding of terrorists has been the Al-Haramain Islamic Foundation (AHF), a charity widely believed to be corrupted by **Al Qaida** and to provide support to other terrorists and terrorist activity. See The 9/11 Comm'n Report: Final Report of the National Comm'n on Terrorist Attacks Upon the United States, at 170 (citing "the Saudi-based al Haramain Islamic Foundation" as an example of a "corrupt" charity infiltrated by **Al Qaida**).

(U) In the U.S. Government's overall efforts to combat terrorist abuse of charities, AHF loomed as a major concern. As noted in a June 2004 Treasury press release announcing AHF-related designations, "When viewed as a single entity, [AHF] is one of the principal Islamic NGOs providing support for the **Al Qaida** network and promoting militant Islamic doctrine worldwide.... Terrorist organizations designated by the U.S. including **Jemmah Islammiya, Al-Ittihad Al-Islamiya, Egyptian Islamic Jihad, HAMAS and Lashkar E-Taibah** received funding from [AHF] and used [AHF] as a front for fundraising and operational activities." [Source: U.S. Department of Treasury, Press Room, June 2, 2004, Exhibit 137]

([redacted] A few instances of AHF's global support for, and ties to, terrorist organizations illustrate the grounds for the U.S. Government's serious concern:[3]

- As early as 1997, U.S. and other authorities were informed that **AHF-Kenya** was involved in plotting terrorist attacks against Americans. As a result, a number of individuals connected to **AHF-Kenya** were arrested and later deported by Kenyan authorities. In August 1997, an **AHF-Kenya** employee indicated that the planned attack against the U.S. Embassy in Nairobi would be a suicide bombing carried out by crashing a vehicle into the gate at the Embassy. A wealthy AHF official outside East Africa agreed to provide the necessary funds. [Source: U.S. Department of Treasury, Press Room, January 22, 2004, Exhibit 99; [redacted]
- A former **AHF-Tanzania** Director, believed to be associated with **Usama bin Ladin**, was responsible for making preparations for the advance party that planned the August 7, 1998, bombings of the U.S. Embassies in Dar Es Salaam, Tanzania, and Nairobi, Kenya, which together killed 224 people. Shortly before the bombing attacks, a former **AHF-Tanzania** official met with another conspirator to the attacks and cautioned the individual against disclosing knowledge of preparations for the attacks. [Source: U.S. Department of Treasury, Press Room, January 22, 2004, Exhibit 99; [redacted]

[3] (U) The press releases cited above were issued on occasion of the designation, pursuant to E.O. 13224, of various AHF branches around the world. The press releases set forth declassified summaries of some of the evidence supporting those designations. The underlying evidence itself is contained in OFAC's files, in the administrative records for those designations.

- A senior AHF official deployed a Bangladeshi national to conduct surveillance on U.S. consulates in India for potential terrorist attacks. The Bangladeshi national was arrested in early 1999 in India, reportedly carrying four pounds of explosives and five detonators. The terrorist suspect told police that he intended to attack U.S. diplomatic missions in India. The suspect reportedly confessed to training in **Al Qaida** terrorist camps in Afghanistan, where he met personally with **Usama bin Ladin** in 1994. The suspect first heard of plans for these attacks at the AHF office in Bangladesh. [Source: U.S. Department of Treasury, Press Room, June 2, 2004, Exhibit 137; [redacted]

- [redacted] **MK,** co-founded and financed by **Usama bin Ladin (UBL)**, is an SDGT pursuant to the authorities of E.O. 13224 and the pre-cursor organization of **Al Qaida**. [Source: United States of America - against- Mohammed Ali Hasan Al-Moayad, Affidavit in Support of Arrest Warrant, Exhibit 70] [redacted]

- Using a variety of means, AHF has provided financial support to **Al Qaida** operatives in Indonesia and to its Southeast Asia affiliate, **Jemaah Islamiyah** (JI). According to a senior **Al Qaida** official apprehended in Southeast Asia, Omar al-Faruq, AHF was one of the primary sources of funding for **Al Qaida** network activities in the region. **JI** has committed a series of terrorist attacks, including the bombing of a nightclub in Bali on October 12, 2002 that killed 202 and wounded over 300. [Source: U.S. Department of Treasury, Press Room, January 22, 2004, Exhibit 99]

([redacted]

[redacted]The United States sought to impede AHF's funding of terrorist groups through both diplomacy, particularly through joint action with Saudi Arabia [Source: Federal News Service, June 2, 2004, Exhibit 135], and through direct regulatory action, i.e. by designating officials and branches of the organization pursuant to E.O. 13224. [redacted]

[redacted]

(S [redacted] On March 11, 2002, the United States and Saudi Arabia took coordinated blocking actions against the **Al Qaida**-affiliated **AHF offices** in **Bosnia** and **Somalia**. [Source: U.S. Department of Treasury, Press Room, March 11, 2002, Exhibit 24][4] [redacted] on January 22, 2004, Saudi Arabia joined with the United States and designated additional **AHF offices** in **Indonesia, Kenya, Tanzania,** and **Pakistan**.[5] These actions were based on evidence that AHF provided support to Specially Designated Global Terrorist organizations including **Al Qaida, Jemaah Islamiyah, Al-Ittihad al-Islamiyya** (**AIAI**) and others. [Source: U.S. Department of Treasury, Press Room, January 22, 2004, Exhibit 99]

(S [redacted] Continuing coordinated efforts, on June 2, 2004, the United States and Saudi Arabia designated additional **AHF offices** in **Afghanistan, Albania, Bangladesh, Ethiopia,** and **The Netherlands**.[6] The U.S. also designated AHF's founder and long-time leader, **Aqeel Abdulaziz Al-Aqil**. These actions were based on evidence that **Al-Aqil** and AHF provided support to Specially Designated Global Terrorist organizations including **Al Qaida, AIAI** and others. [Source: U.S. Department of Treasury, Press Room, June 2, 2004, Exhibit 137] [redacted]

(U) Finally, on September 9, 2004, after consultation with the Secretaries of State and Homeland Security and the Attorney General, OFAC designated **AHF-OREGON** as an SDGT. In the same action, OFAC designated **AHF-OREGON** Director **Soliman AL-BUTHE** (**AL-BUTHE**) and the **AHF branch** in the **Comoros Islands** (**AHF-Comoros Islands**). [Source: U.S. Department of Treasury Press Release, September 9, 2004, Exhibit 221]

[redacted]

[4] (U) The United States designated the **Bosnia** and **Somalia** offices pursuant to the authorities of E.O. 13224.

[5] (U) The designations were made pursuant to E.O. 13224.

[6] (U) The designations were made pursuant to E.O. 13224.

[7] (U) These reported actions comport with official stated Saudi policy regarding Non-Governmental Organizations (NGOs). On June 2, 2004, the Adviser to Saudi Crown Prince Abdullah stated that existing entities, including AHF, would be dissolved or have their assets folded into the Saudi National Entity for Charitable Work Abroad. The Adviser explained that the Saudi National Entity for Charitable Work Abroad would be the sole vehicle through which all private Saudi donations will go to help those in need. According to the Saudi advisor, the purpose of this effort was to put in place new regulations and financial control mechanisms to ensure that people "don't take advantage of our financial system or of our charities." [Source: Federal News Service, June 2, 2004, Exhibit 135]

[redacted]

[redacted]

(U) AHF AS A GLOBAL ENTERPRISE

[redacted]

(S)[redacted] Yet according to a Saudi news report, **Al-Aqil** reportedly stated, "I resigned willingly. I wanted to give new blood a chance to assume the responsibilities, since I have personal business that I need to attend to. I have not left the organization, I have just resigned as General Manager, I will stay on as an active member and as an advisor," [redacted] **Al-Aqil** had reportedly been the head of AHF for many years and was one of AHF's founders, [redacted] [Source: RIYADH 000164, Exhibit 72; See also, FBIS, London Al-Hayah in Arabic, January 8, 2004, Exhibit 104]

(S[redacted] Among the reasons for **Al-Aqil's** removal was his "absolute centralization" of AHF, according to a Saudi news report. [Source: FBIS, London Al-Hayah in Arabic, January 8, 2004, Exhibit 104] Mansour Al-Kadi, [redacted] cited **Al-Aqil's** "autocratic and centralist governance" of AHF as the main reason for his resignation, according to an Arabic language posting on an Internet forum. [redacted] the Internet posting identifies **Al-Aqil** as the "only individual with final decision making on

---

[redacted]

10 (S[redacted] AHF-OREGON Tax Form 990, 2001, Exhibit 39; [redacted]

spending…and the one with the authority to hire employees, even if it is just a janitor." [Source: http://alsaha.fares.net/, Exhibit 106]

(U) **Al-Aqil** himself responded to an Arab news outlet question regarding the extent to which AHF maintains "tight control over the affiliated offices" by stating: "Yes, of course. The offices' directors are employees who follow the directions of the main office with regards to hiring workers at the offices and making any decisions on cooperation with any party. In the main office, there are 19 auditors. Each of the foundation's specialized committees has an auditor. There are monthly, quarterly, and yearly reports on the foundation's revenue and expenditure." [Source: Open Source Center, London Al-Sharq al-Awsat, March 16, 2002, Exhibit 153]

(U) As set forth below, the AHF headquarters, under **Al-Aqil's** leadership, provided funding and instructions that governed the activities of AHF throughout the world including in Bosnia, Albania, Iraq, the United States, and elsewhere.

[redacted]

[12] (U) **AHF-Bosnia** was designated on March 11, 2002 pursuant to the authorities of E.O. 13224. [Source: U.S. Department of Treasury, Press Room, March 11, 2002, Exhibit 24]

[13] (U) Subsequent to its designation, **AHF-Bosnia** reopened under the name **Vazir**. On December 22, 2003, **Vazir** was designated pursuant to the authorities of E.O. 13224. Saudi Arabia joined the U.S. to request that the UN 1267 Sanctions Committee also list **Vazir**. [Source: U.S. Department of Treasury, Press Room, December 22, 2003, Exhibit 98]

[redacted]

(S[redacted]

As of March 2004, **Al-Aqil**, and his deputy Mansour Al-Kadi, were identified as board members of **AHF-The Netherlands**, according to diplomatic reporting. [Source: THE HAGUE 000771, Exhibit 108]

[redacted]

(U) ADDITIONAL AHF-RELATED INFORMATION

[redacted]

[14] (U) On June 2, 2004, the Adviser to Saudi Crown Prince Abdullah stated that existing entities, including AHF, will be dissolved or have their assets folded into the Saudi National Entity for Charitable Work Abroad. The Adviser explained that the Saudi National Entity for Charitable Work Abroad will be the sole vehicle through which all private Saudi donations will go to help those in need. According to the Saudi Adviser, the purpose of this effort is to put in place new regulations and financial control mechanisms to ensure that people "don't take advantage of our financial system or of our charities." [Source: Federal News Service, June 2, 2004, Exhibit 135]

[redacted]

(U) ACTIONS OF CERTAIN AHF BRANCHES THROUGHOUT THE WORLD

[redacted]

(U) ALBANIA

(S [redacted] In 1998, the head of **Egyptian Islamic Jihad (EIJ)** in Albania was reportedly also the "accountant" for **AHF-Albania,** according to a French news report. [Source: FBIS, Paris Le Figaro in French, September 30, 1998, Exhibit 91] This individual, Ahmed Ibrahim al-Nagar, was reportedly extradited from Albania to Egypt in 1998. At his trial in Egypt, al-Nagar reportedly voiced his support for **UBL** and **Al Qaida's** terrorist attacks against the U.S. Embassies in Tanzania and Kenya, according to Agence France Presse. [Source: Agence France Presse, February 1, 1999, Exhibit 93]

(S [redacted] Institute for War and Peace Reporting, January 31, 2003, Exhibit 101]

[redacted]

[redacted]

(U) KOSOVO

[redacted]

(U) IRAQ

[redacted]

[16] (U) The **National Liberation Army** is designated pursuant to the authorities of E.O. 13304.

(U) SOMALIA

[redacted]

(U) UNITED STATES **(AHF-OREGON)**

(U) On the U.S. **AHF-OREGON's** tax form 990 for 2001 filed with the IRS, **Al-Aqil** is identified as the President, Al-Kadi as the Vice President, **AL-BUTHE** as the Treasurer, and Perouz Seda Ghaty (Seda) as the Secretary. [Source: **AHF-OREGON** Tax Form 990, 2001, Exhibit 39] The **AHF-OREGON** branch's Articles of Incorporation and application to the IRS for tax-exempt status also list **Al-Aqil**, Al-Kadi, Seda, and **AL-BUTHE** as members of the board of directors. [United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95] Seda also is identified as the registered agent for

**AHF-OREGON** and as a member of the board of directors of **AHF-OREGON**, according to an Affidavit filed in federal court in the U.S. [United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95] **AHF-OREGON** appeared to first establish its presence in the U.S. when Seda and **AL-BUTHE** registered the organization with the Oregon Secretary of State as an assumed business name in October 1997. [United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95]

[redacted]

(S[redacted]During April 1999, Seda allegedly announced during a prayer session that he was outraged at atrocities in Kosovo carried out by the Serbian military against Muslims. Seda reportedly announced during the same session that he knew of mujahideen willing to travel to the region to fight Serbs, and then reportedly began to solicit funds for the same. [Source: U.S. v. Perouz Sedaghaty aka Pete Seda, [No. CR 05-60008-01], the Government Memorandum in Support of Pretrial Detention, (Pretrial Detention Request) August 21, 2007, and accompanying exhibits A-P, Exhibit 156] That same month, Seda wired $2,000 to the **AHF office in Albania.** [Source: Pretrial Detention Request exhibit K, Exhibit 212] The **AHF-Albania** office was the closest AHF office to the fighting in Kosovo.[17] [Source: Pretrial Detention Request, Exhibit 156][18] [redacted]

(TS[redacted]In late 2001, Seda, a senior AHF official in the U.S., sought a license from OFAC to purportedly assist Afghan refugees in border camps in Iran on the Iranian/Afghanistan border. [Source: Correspondence from Perouz Seda Ghaty to the OFAC Licensing Division, November 1, 2001, Exhibit 37] As part of Seda's request to OFAC in November 2001,[19] he reported that **Shaykh Al-Aqil**, identified as the President of AHF, agreed to Seda's proposal to fund $500,000 for assistance to Afghan refugees in border camps in Iran. [redacted]

[17] (U) As noted elsewhere in this memorandum, the **AHF-Albania** branch was designated as an SDGT on June 2, 2004. See, Exhibit 137.

[redacted]

[19](U) [Source: Correspondence from Perouz Seda Ghaty to the OFAC Licensing Division, November 1, 2001, Exhibit 37]

[redacted]

(U) As of March 2003 **Al-Aqil** and Al-Kadi reportedly resigned from the **AHF-OREGON** office. [Source: Correspondence from Bernabei & Katz, PLLC to OFAC, August 4, 2004, (AHF Counsel Exhibits 1 and 2), Exhibit 151]

(U) On February 18, 2004, Federal law enforcement authorities executed a search warrant against property purchased on behalf of AHF in Ashland, Oregon. The search was conducted pursuant to a criminal investigation into possible violations of the Internal Revenue Code, the Money Laundering Control Act and the Bank Secrecy Act. In a separate administrative action, OFAC blocked pending investigation AHF accounts and real property in the U.S. to ensure the preservation of AHF assets pending further investigation. [Source: U.S. Department of Treasury, Press Room, February 19, 2004, Exhibit 94; United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95]

(U) ADDITIONAL INFORMATION

(U) In support of the request for reconsideration of the designation of **AL-BUTHE, AL-BUTHE** counsel informed OFAC via correspondence that **AL-BUTHE** learned during March 2000 "while en route to the United States" that a Dr. Mahmoud El-Fiki "had contributed $150,000 to [**AHF-OREGON**], designating it for Chechen relief efforts." [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154] As indicated in Exhibit 95 (the United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant), documents referenced in the exhibit include the February 21, 2000 letter from **Al-Aqil** to Fiki in which **Al-Aqil** himself thanked Fiki for his "generous donation of $150,000." [Source: United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95]

(U) In March 2000, **AL-BUTHE** and **AHF-OREGON** official Seda were involved with withdrawing the $150,000 Fiki contribution from the **AHF-OREGON** branch bank account, after which **AL-BUTHE** transported the funds in travelers' checks and a cashier's check from the United States to Saudi Arabia. The indictment of **AL-BUTHE**, Seda and **AHF-OREGON** indicates the following in regards to Fiki's donation: "Intending that the funds be delivered to the Chechen mujahideen, defendants Pirouz Sedagaty [Seda], **Soliman** [**AL-BUTHE**], the [**AHF-OREGON**], and others, engaged in a conspiracy to prevent the United States Government from learning of the transaction by failing to fill out paperwork, as required by law, acknowledging the funds were leaving the United States, and by filing a false tax return with the Internal Revenue Service which falsified how the donated funds were distributed by defendant [**AHF-OREGON**]." [Source: Copy of Indictment in U.S. v. AL-HARAMAIN ISLAMIC FOUNDATION, INC.; Pirouz SEDAGHATY, a/k/a Pete Seda, Perouz Seda Ghaty and Abu Yunus; and Soliman Hamd **AL-BUTHE**, Exhibit 165]

[redacted]

[20] (U) The Russian Federal Security Service, which was reported to have been monitoring AHF activities since 1999, identified a bank account through which some $1 million reportedly was sent for weapons and terrorists, and determined that Mansur Bin Abd al-Rakhman Al-Kadi sent 480,000 Saudi Rials through AHF channels to Chechen separatists. [Source: Open Source Center, Milan Panorama, November 27, 2003, Exhibit 199]

(U) [redacted] The 479,514 Saudi Rial receipt reportedly accounts for part of the Fiki-donated $150,000 donated by Fiki and carried by **AL-BUTHE** from Oregon to Saudi Arabia. [Source: Exhibit L of the Pretrial Detention Request, Exhibit 210; and correspondence from AHF attorney Lynne Bernabei to OFAC, February 14, 2005, with attachments, Exhibit 200]

[redacted]

[21] (S [redacted] Khattab and Chechen terrorist **Shamil Basayev** together led the **Islamic International Brigade.** Basayev's forces led the August 1999 incursion into Daghestan which by late September 1999 helped precipitate the second Chechen war. [Source: "Terrorist Designation Under Executive Order 13224 **Islamic International Brigade, Special Purpose Islamic Regiment,** and **Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs,**" U.S. Department of State, February 28, 2003; and Appendix C of the 2003 Patterns of Global Terrorism Report, U.S. Department of State, collectively Exhibit 158; Washington Post, March 20, 2000, Exhibit 219]

(S[redacted] as indicated by the United States Department of State during February 2003, Khattab and **Shamil Basayev** together headed the **Islamic International Brigade, (IIB)**. The **IIB** was one of three **Al-Qaida**-linked and Chechnya-based terrorist organizations designated as Specially Designated Global Terrorists on February 14, 2003 for involvement in the Dubrovka Theater seizure in Moscow during October 2002. Some 129 persons were killed in the attack, including one U.S. citizen.[23] [Source: "Terrorist Designation Under Executive Order 13224 **Islamic International Brigade, Special Purpose Islamic Regiment**, and **Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs**," U.S. Department of State, February 28, 2003; and Appendix C of the 2003 Patterns of Global Terrorism Report, U.S. Department of State, collectively Exhibit 158]

(U) Documents and other materials (e.g. the aforementioned videos) relating to Chechnya and Chechen mujahideen were obtained by law enforcement officials from **AHF-OREGON** and/or from **AHF-OREGON** office computers in late 2003/early 2004. Among photographs seized in February 2004 was one of Islamic Army of the Caucasus (IAC) Commander in Chief **Shamil Basayev**,[24] together with Ibn Ul Khattab of the IAC-loyal Foreign Mujahideen Brigade, and Khattab's successor (Khattab was killed in March 2002), Abu Al-Walid Al-Ghamidi. [Source: Accompanying exhibit H of the Pretrial Detention Request, Exhibit 211] The Pretrial Detention Request also indicates that videos seized from **AHF-OREGON** depict violent acts committed

[redacted]

[23] (U) The **IIB**, the **Special Purpose Islamic Regiment**, and the **Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs** were together added to the UN 1267 list on March 4, 2003; **Shamil Basayev** was added to the UN 1267 list on August 12, 2003. [Source: Copy of portions of the 1267 Consolidated List of the United Nations Security Council's **Al Qaida** And Taliban Sanctions Committee noting the March 4, 2003 addition of the **Islamic International Brigade, Special Purpose Islamic Regiment**, the **Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs**, and the August 12, 2003 addition of **Shamil Basayev**, Exhibit 218] These groups were submitted for designation to the UN Sanctions Committee by the five permanent members of the UN Security Council, and Spain and Germany – "the first time that the permanent members made such a joint submission on a terrorist designation." [Source: "Eurasia Overview" of the 2003 Patterns of Global Terrorism Report, U.S. Department of State, Exhibit 217]

[24] (U) **Shamil Basayev** was designated as an SDGT on August 8, 2003.

against Russian soldiers by mujahideen in Chechnya. Among the items found on Seda's computer were photographs of deceased mujahideen and Russian soldiers, passports belonging to deceased Russian soldiers, and a map indicating the location of mujahideen military engagements. [Source: Accompanying exhibit G of the Pretrial Detention Request, Exhibit 157]

(U) COMOROS ISLANDS, ETHIOPIA, and BANGLADESH

[redacted]

(U) IRAN

[redacted]

[26] (S) The following sources include additional information on Al Qaida and other activities of concern in the Comoros. [redacted] United States of America v. Usama Bin Laden, et al., trial transcript, May 2, 2001, Exhibit 140; United States of America v. Usama Bin Laden, et al., trial transcript, May 7, 2001, Exhibit 141; United States of America v. Usama Bin Laden, et al., trial transcript, May 8, 2001, Exhibit 142]

[redacted]

[redacted]

(U) SENIOR AHF OFFICALS

(S [redacted] Information on additional senior AHF officials is set forth below.

(U) **Aqeel Abdelaziz Al-Aqil**

(S [redacted] The New York Times, September 26, 2003, Exhibit 102] **Al-Aqil** was designated pursuant to the authorities of E.O. 13224 on June 2, 2004. [redacted] **Al-Aqil** also is identified as AHF's President and Chairman. [Source: **AHF-OREGON** Tax Form 990, 2001, Exhibit 39; The Sunday Oregonian, November 9, 2003, Exhibit 103; FBIS, London Al-Hayah in Arabic, March 1, 2004, Exhibit 105]

(S) [redacted] According to a Saudi news report, **Al-Aqil** reportedly stated, "I resigned willingly. I wanted to give new blood a chance to assume the responsibilities, since I have personal business that I need to attend to. I have not left the organization, I have just resigned as General Manager, I will stay on as an active member and as an advisor," [redacted] **Al-Aqil** reportedly had been the head of AHF for many years. [Source: RIYADH 000164, Exhibit 72; See also, FBIS, London Al-Hayah in Arabic, January 8, 2004, Exhibit 104]

(S [redacted] Among the reasons for **Al-Aqil's** removal was his "absolute centralization" of AHF, according to a Saudi news report. [Source: FBIS, London Al-Hayah in Arabic, January 8, 2004,

[redacted]

Exhibit 104] Mansour Al-Kadi, [redacted] cited **Al-Aqil's** "autocratic and centralist governance" of AHF as the main reason for his resignation, according to an Arabic language posting on an Internet forum. [redacted] the Internet posting identifies **Al-Aqil** as the "only individual with final decision making on spending…and the one with the authority to hire employees, even if it is just a janitor." [Source: http://alsaha.fares.net/, Exhibit 106]

[redacted]

(U) Additional **Aqeel Abdelaziz Al-Aqil** Information

[redacted]

[29] (S [redacted] **AHF-OREGON** Tax Form 990, 2001, Exhibit 39 [redacted]

[redacted]

(U) Mansour bin Abdul Rahman Al-Kadi

(S) [redacted] RIYADH 001094, Exhibit 47; **AHF-OREGON** Tax Form 990, 2001, Exhibit 39 [redacted]

(U) Additional Information on Mansur bin Abdul Rahman Al-Kadi

[redacted]

(S[redacted] Hisham Al-Mashari

[redacted]

[36] (U) **AHF-Bosnia** was designated on March 11, 2002 pursuant to the authorities of E.O. 13224. [Source: U.S. Department of Treasury, Press Room, March 11, 2002, Exhibit 24]
[37] (U) Subsequent to the designation of **AHF-Bosnia**, it reopened under the name **Vazir**. On December 22, 2003, **Vazir** was designated pursuant to the authorities of E.O. 13224. Saudi Arabia joined the U.S. to request that the UN 1267 Sanctions Committee also list **Vazir**. [Source: U.S. Department of Treasury, Press Room, December 22, 2003, Exhibit 98]

[redacted]

(U) **Soliman AL-BUTHE**

(U) **AL-BUTHE** has been identified as the Treasurer of **AHF-OREGON**, according to the U.S. **AHF-OREGON** tax form 990 for 2001 filed with the IRS. [Source: **AHF-OREGON** Tax Form 990, 2001, Exhibit 39] Resident in Riyadh, Saudi Arabia, **AL-BUTHE** also reportedly assisted in the establishment of **AHF-OREGON**, and served as the chairman of AHF's U.S. Committee, according to an Affidavit in Support of an Application for Search Warrant and local news reports. [Source: United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95; The Oregonian, January 10, 2004, Exhibit 121; The Sunday Oregonian, November 9, 2003, Exhibit 103] In a document signed by **AHF's** leader **Al-Aqil**, AHF in Saudi Arabia appointed **AL-BUTHE** "true and lawful attorney in [AHF's] name, place and stead," apparently giving **AL-BUTHE** broad legal authority to act on AHF's behalf in the U.S. [United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95]

(S [redacted] [Source: Knight Ridder/Tribune News Service, June 3, 2003, Exhibit 123; [redacted] **AL-BUTHE's** role as a senior AHF official is corroborated in part by information obtained by the FBI. A letter drafted on AHF "head office-Riyadh" stationery identifies **AL-BUTHE** as the President of AHF's Internet Committee. [Source: Copy of Government Exhibit F139a, Exhibit 127]

(U) Other evidence shows that **AL-BUTHE** had signature authority to sign contracts on behalf of AHF's head office in Riyadh, Saudi Arabia. On or about February 15, 2002, a "Memorandum of Agreement" showed that **AL-BUTHE** represented AHF in an agreement that was signed with a U.S. party for the development and distribution of religious materials. [Source: Government Exhibit F67A, Exhibit 128] In two other related contracts, **AL-BUTHE** also represented AHF in signing agreements. [Source: Copy of Government Exhibit F61A, Exhibit 129; E010(4B36-31-098 to 100), Exhibit 130]

[redacted]

(U) On February 18, 2004, Federal law enforcement authorities executed a search warrant against property purchased on behalf of **AHF-OREGON**. The search was conducted pursuant to a criminal investigation into possible violations by **AL-BUTHE** (and Seda) of the Internal Revenue Code, the Money Laundering Control Act and the Bank Secrecy Act. In a separate administrative action, OFAC blocked pending investigation AHF accounts and real property in the U.S. to ensure the preservation of AHF assets pending further investigation. [Source: U.S. Department of Treasury, Press Room, February 19, 2004, Exhibit 94; United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95]

[redacted]

(U) Additional Information on **Soliman AL-BUTHE**

[redacted]

(U//FOUO) **AL-BUTHE** and Seda were involved with the withdrawal of funds from the **AHF-OREGON** branch office bank account during March 2000. The withdrawn funds included a $150,000 contribution from Dr. Mahmoud Talaat El-Fiki. In a February 20, 2000 email to "haramain" notifying the organization of Fiki's contribution it was indicated that the money was given "as Zakat in order to participate in your noble support to our muslim brothers in Chychnia."[39] Also noted in the email was "our previous correspondence," and the fact that a request was made to Fiki's bank in London "to make a transaction to your USA account, *using*

[redacted]

*the details you provided in an earlier email...,*" (emphasis added). The money subsequently was transported by **AL-BUTHE** to Saudi Arabia, at which point it is believed to have been sent to mujahideen in Chechnya. [Source: Pretrial Detention Request, Exhibit 156; Accompanying exhibit L of the Pretrial Detention Request, Exhibit 210]

(U) In support of the request for reconsideration of the designation of **AL-BUTHE, AL-BUTHE** counsel informed OFAC via correspondence that **AL-BUTHE** first learned of Fiki's contribution during early March 2000 – this despite the February 20, 2000 Fiki-related email which referenced "previous correspondence" and "details...provided in an earlier email." [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; accompanying exhibit L of the Pretrial Detention Request, Exhibit 210] The attorney correspondence also indicated that "**AL-BUTHE** is uncertain why Dr. Fiki (whom Mr. **AL-BUTHE** has never met) sent the contribution to the United States instead of Saudi Arabia," but **AL-BUTHE** "speculates that there probably are fewer restrictions on [affecting] such transfers into the United States." **AL-BUTHE** also speculated that Fiki may have responded to "website instructions or advertisements that had been published in Islamic magazines directing contributions to the United States." That speculation, however, appears inconsistent with the aforementioned reference to "previous correspondence" and with the fact that Fiki's contribution to the U.S. bank account was completed "using details...provided in an earlier email." [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; accompanying exhibit L from the Pretrial Detention Request, Exhibit 210]

(TS[redacted]In support of the request for reconsideration of the designation of **AL-BUTHE, AL-BUTHE** counsel also informed OFAC via correspondence that **AL-BUTHE** worked on the Saudi-based AHF website as early as 1993, and continued in this work as late as March 2000. Moreover, the letter indicated that the very purpose of **AL-BUTHE's** trip to the United States during March 2000 was to assist "in establishing an Islamic website, IslamToday."[40] Additionally, it is elaborated in the correspondence that **AL-BUTHE's** role with the AHF evolved over time to the point at which he became "responsible for internet activities and then for charitable works in the United States."[41] [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154] According to the indictment of Seda and **AL-BUTHE**, the AHF website (www.alharamain.org), as of 1999 and 2000, contained numerous articles supportive of the Chechen mujahideen, to include reports such as "The Latest News About Jihaad in Chechnya." The website also contained a prayer for Chechen mujahideen, referring to them as the "Mujahideen brothers in Chechnya." The indictment further indicates that a link was provided via the AHF website to www.qoqaz.com, through which details could be obtained on how to fund Chechen mujahideen.[42] [Source: Copy

[40] (U) The March 2000 trip referenced here is the same trip during which Fiki's $150,000 contribution was withdrawn from the **AHF-OREGON** account and transported by **AL-BUTHE** from the United States to Saudi Arabia. [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154]

[redacted]

of Indictment in U.S. v. AL-HARAMAIN ISLAMIC FOUNDATION, INC.; Pirouz SEDAGHATY, a/k/a Pete Seda, Perouz Seda Ghaty and Abu Yunus; and Soliman Hamd **AL-BUTHE**, Exhibit 165] Thus, an argument that **AL-BUTHE** was ignorant of AHF facilitation (e.g. via qoqaz.com) of funding of the Chechen mujahideen would be questionable given his internet-related responsibilities, his overt acts (transporting the $150,000 Fiki contribution), his official position with the AHF and its Oregon branch (supportive of Chechen mujahideen). [redacted] [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; letter presumably from **AL-BUTHE** identifying him as the President of the "Internet Committee" of AHF-Riyadh, Exhibit 127; copy of Indictment in U.S. v. AL-HARAMAIN ISLAMIC FOUNDATION, INC.; Pirouz SEDAGHATY, a/k/a Pete Seda, Perouz Seda Ghaty and Abu Yunus; and Soliman Hamd **AL-BUTHE**, Exhibit 165; [redacted]

[redacted]

([redacted] Intercepts disclosed during Al-Timimi's trial (Al-Timimi was [redacted] convicted and sentenced to life in prison) reveal a relationship between Al-Timimi and **AL-BUTHE**. **AL-BUTHE** was intercepted in some four conversations with Al-Timimi. In an intercept on February 1, 2003, at 15:38 Al-Timimi spoke with FNU LNU,[46] (subsequently determined to be **Soliman AL-BUTHE**). [**Source**: Copy of United States of America v. Ali Al-Timimi, United States District Court for the Eastern District of Virginia, Exhibit 168; Stipulations 17-24, United States District Court for the Eastern District of Virginia, Exhibit 204] During the conversation, FNU LNU provided Al-Timimi with the following fax number: 966-12066331. During the same intercept, FNU LNU passed the telephone to Ahmad LNU. After a brief conversation, Al-Timimi told Ahmad LNU to ask "Sulayman," (likely **Soliman AL-BUTHE**) to call him (Al-Timimi) the next day so that Al-Timimi could dictate something to "Sulayman." That same day at 16:20 Al-Timimi again was intercepted speaking to FNU LNU (subsequently determined to be **Soliman AL-BUTHE**). [**Source**: GX 10B4A, Copy of Ali Al-Timimi Telephone Intercept Linesheet, Exhibit 206; Stipulations 17-24, United States District Court for the Eastern District of Virginia, Exhibit 204] During the conversation FNU LNU provided Al-Timimi with the following U.S. telephone (probable fax) number: 253-981-9150. An internet query links both aforementioned telephone numbers with ICSFP.com and sb@whymuhammad.net. The latter internet addresses, per the Internet search, correspond both to the International Committee for the Support of the Final Prophet (ICSFP) and the Office of the Campaign to Defend the Prophet. The query also indicates that **AL-BUTHE** is the President of the ICSFP. [Source: Internet query printout relating to telephone numbers 966-120066331 and 253-981-9150, Exhibit 207]

[redacted]

[46] (U) GX 10B3A, Copy of Ali Al-Timimi Telephone Intercept Linesheet, Exhibit 205. "FNU LNU" refers to First Name Unknown, Last Name Unknown.

[redacted]

(U) CONCLUSION

(U) **AL-BUTHE** should be determined to be subject to Executive Order 13224 for the following reason:

- By serving as a senior AHF official, **AL-BUTHE** has acted for or on behalf of, has assisted in, sponsored, or provided financial, material, or technological support for, or financial or other services to or in support of **Al Qaida** and other SDGTs.

(U) **AHF-OREGON** should be determined to be subject to Executive Order 13224 for the following reasons:

- **AHF-OREGON** has been owned or controlled by, or has acted for or on behalf of **Al-Aqil**.
- **AHF-OREGON** has been owned or controlled by, or has acted for or on behalf of **AL-BUTHE**.
- As a branch of the Saudi charity Al-Haramain Islamic Foundation, **AHF-OREGON** has acted for or on behalf of, or has assisted in, sponsored, or provided financial, material, or technological support for, or financial or other services to or in support of **Al Qaida** and other SDGTs.

[redacted]